(19)日本国特許庁（ＪＰ）　(12) **公表特許公報（Ａ）**　(11)特許出願公表番号

特表平6－500900

第７部門第３区分　(43)公表日　平成６年(1994)１月27日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ
Ｈ０４Ｂ	7/26	１０９ Ｓ	7304－5K	
Ｈ０４Ｌ	9/06			
	9/14			
Ｈ０４Ｑ	7/04	Ｄ	7304－5K	
			7117－5K	
				Ｈ０４Ｌ 9/02 Ｚ

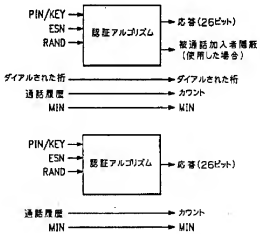
審査請求　有　予備審査請求　有　（全 26 頁）

(21)出願番号　特願平3－514449
(86)（22)出願日　平成３年(1991)７月18日
(85)翻訳文提出日　平成５年(1993)１月22日
(86)国際出願番号　ＰＣＴ／ＵＳ９１／０５０７８
(87)国際公開番号　ＷＯ９２／０２０８７
(87)国際公開日　平成４年(1992)２月６日
(31)優先権主張番号　５５６，８９０
(32)優先日　1990年７月23日
(33)優先権主張国　米国（ＵＳ）
(81)指定国　ＡＵ，ＣＡ，ＧＢ，ＪＰ，ＫＲ

(71)出願人　エリクソン　ジーイー　モービル　コミュニケーションズ　インコーポレイテッド
アメリカ合衆国22709　ノース　カロライナ州　リサーチ　トライアングル　パーク，トライアングル　ドライブ　１，ピー．オー．ボックス　13969
(72)発明者　デント，ポール，ウィルキンソン
スウェーデン国エス　－　240　36　ステハグ，ステハグス　プラストガールド（番地なし）
(74)代理人　弁理士　浅村　皓　（外２名）

(54)【発明の名称】　デジタルセルラ通信用認証システム

(57)【要約】
セルラ通信ネットワークにおける、移動局と基地局の認証のためのシステム。前記システムは、ランダム挑戦に対するキー依存応答だけでなく、ネットワーク内のトラッフィックを暗号化するために用いることができる、一時的会話キーまたは通話変数も発生するアルゴリズムを備えている。ネットワークにおいてクローンに対して防御するために、前記アルゴリズムは、履歴情報を含むローリングキーを用いる。両方向認証手順を用いて、ローリングキーを更新し、そして新しい会話キーを発生することができる。



請求の範囲

1．デジタルセルラ通信システムにおける通信の機密性を強化するために用いられる複数のパラメータの発生のための方法であって、各移動局には唯一の多数桁秘密永久キーが割り当てられ、定期的に変化する多数桁ローリングキーが機密性を高めるために用いられており、前記永久キーと前記ローリングキーの両方は、各移動局と移動のホームネットワークに記憶されており、

ある位置で、訪問先ネットワークからのランダム認証問い合せを表わす信号と、特定の移動局を表わす信号とを含む、複数の多数桁入力信号を、前記特定の移動局の多数桁永久キー及び前記特定の移動に関連した多数桁ローリングキーと共に、その特定の時刻に受信し、

前記入力信号の桁を第1の集合（ｇｒｏｕｐｉｎｇ）に構成し、

前記入力信号の第1の集合と前記永久及びローリングキーの桁から、第1のアルゴリズムにしたがって、第1の出力値を計算し、

前記第1の出力値を含む桁の連続的に構成したブロックを、訪問先ネットワークによる認証の問い合せに対して応答するために、前記移動局によって用いられる認証応答と、それを移動局に対して認証するために、訪問先ネットワークによって用いられる認証値号とを含む、前記システム内で用いるための選択されたパラメータに割り当て、

前記入力信号の桁を、第2の集合に構成し、

前記入力信号の第2の集合と、前記永久及びローリングキー桁から、第2のアルゴリズムにしたがって、第2の出力値を計算し、及び

前記第2の出力値を含む桁の連続的に構成したブロックを、システム内で通信データを暗号化するための疑似ランダムビットのキーストリームを計算するために用いられる機密キーと、次の特定時刻に特定な移動と関連する新しいローリングキーとを含む、前記システム内で用いるための選択したパラメータに割り当る、

ことから成る、前記方法。

2．請求項1記載のデジタルセルラ通信システムにおいて通信の機密性を強化するために用いられる複数のパラメータの発生のための方法において、

前記第1の出力値を含む前記桁の連続的に構成されたブロックが割り当てられる、前記システム内で用いるための出力パラメータは、移動局によって送信された通話された番号を確認するために用いられる信号も含んでいる、前記方法。

3．請求項1記載のデジタルセルラ通信システムにおいて~~システムにおいて~~通信の機密性を強化するために用いられる複数のパラメータの発生のための方法において、前記第1及び第2のアルゴリズムは、コードループの繰り返し実行を含んでいる、前記方法。

4．請求項1記載のデジタルセルラ通信システムにおいて通信の機密性を強化するために用いられる複数のパラメータの発生のための方法において、前記第1及び第2のアルゴリズムは、入力信号及びキー桁のバイトの先々の対が繰り返し互いに排算される、混合通過を構えている、前記方法。

5．請求項1記載のデジタルセルラ通信システムにおいて~~デジタルセルラ通信システムにおいて~~通信の機密性を強化するために用いられる複数のパラメータの発生のための方法において、前記方法は、各移動局のホーム交換において実行される、前記方法。

6．請求項4記載のデジタルセルラ通信システムにおいて通信の機密性を強化するために用いられる複数のパラメータの発生のための方法において、前記第1のアルゴリズムにしたがった計算は、前記入力信号及び前記ローリングキー桁を含む一連のバイトを集合化し、そして、その先々のバイトを第1の順序で配置された前記永久キーのバイトと加算によって混合することを含んでいる、前記方法。

7．請求項5記載のデジタルセルラ通信システムにおいて通信の機密性を強化するために用いられる複数のパラメータの発生のための方法において、前記第2のアルゴリズムにしたがった計算は、前記入力信号及び前記ローリングキー桁を含む一連のバイトを集合化し、そして、その先々のバイトを前記第1の順序とは異なる第2の順序で配置された前記永久キーのバイトと加算によって混合することを含んでいる、前記方法。

8．請求項4記載のデジタルセルラ通信システムにおいて通信の機密性を強化するために用いられる複数のパラメータの発生のための方法において、各加算から得られた前記値は、その入力及びその出力の間で1：1のマッピングを有する固定参照テーブルから、乱数を得るために用いられる、前記方法。

9．請求項4記載のデジタルセルラ通信システムにおいて通信の機密性を強化するために用いられる複数のパラメータの発生のための方法において、前記固定参照テーブルは、前記システム内で、通信データを暗号化するための疑似ランダムキーストリームを発生するためのアルゴリズムにおいて用いるための、乱数を得るために用いられる、前記方法。

10．デジタルセルラ通信システムにおける通信の機密~~セルラ通信の機密~~性を強化するために用いられる複数のパラメータの発生のためのシステムであって、各移動局には唯一の多数桁秘密永久キーが割り当てられ、定期的に変化する多数桁ローリングキーが機密性を高めるために用いられており、前記永久キーと前記ローリングキーの両方は、各移動局と移動のホームネットワークに記憶されており、

ある位置で、訪問先ネットワークからのランダム認証問い合せを表わす信号と、特定の移動局を表わす信号とを含む、複数の多数桁入力信号を、前記特定の移動局の多数桁永久キー及び前記特定の移動に関連した多数桁ローリングキーと共に、その特定の時刻に受信するための

手段と、

前記入力信号の桁を第１の集合に構成する手段と、

前記入力信号の第１の集合と前記永久及びローリングキーの桁から、第１のアルゴリズムにしたがって、第１の出力値を計算する手段と、

前記第１の出力値を含む桁の連続的に構成したブロックを、訪問先ネットワークによる認証の問い合せに対して返答するために、前記移動局によって用いられる認証応答と、それを移動局に対して認証するために、訪問先ネットワークによって用いられる認証信号とを含む、前記システム内で用いるための選択されたパラメータに割り当てる手段と、

前記入力信号の桁を、第２の集合に構成する手段と、

前記入力信号の第２の集合と、前記永久及びローリングキー桁から、第２のアルゴリズムにしたがって、第２の出力値を計算する手段と、及び

前記第２の出力値を含む桁の連続的に構成したブロックを、システム内で通信データを暗号化するための疑似ランダムビットのキーストリームを計算するために用いられる暗号キーと、次の特定時刻に特定な移動と関連する新しいローリングキーとを含む、前記システム内で用いるための選択したパラメータに割り当る手段と、

ことから成る、前記方法。

１１．請求項１０記載のデジタルセルラ通信システムにおいて通信の機密性を強化するために用いられる複数のパラメータを発生するためのシステムにおいて、前記第１のアルゴリズムにしたがった計算のための手段は、前記入力信号及び前記ローリングキー桁を含む一連のバイトを集合化し、そして、その夫々のバイトを第１の順序で配置された前記永久キーのバイトと加算によって混合する手段を含んでいる、前記システム。

１６．請求項１５記載のデジタルセルラ通信システムにおいて通信の機密性を強化するために用いられる複数のパラメータを発生するためのシステムにおいて、前記第２のアルゴリズムにしたがった計算のための手段は、前記入力信号及び前記ローリングキー桁を含む一連のバイトを集合化し、そして、その夫々のバイトを前記第１の順序とは異なる第２の順序で配置された前記永久キーのバイトと加算によって混合する手段を含んでいる、前記システム。

１７．請求項１３記載のデジタルセルラ通信システムにおいて通信の機密性を強化するために用いられる複数のパラメータを発生するためのシステムにおいて、各加算から得られた前記値は、その入力及びその出力の間で１：１のマッピングを有する固定参照テーブルから、元数を得るために用いられる、前記システム。

１８．請求項１７記載のデジタルセルラ通信システムにおいて通信の機密性を強化するために用いられる複数のパラメータを発生するためのシステムにおいて、前記固定参照テーブルは、前記システム内で、通信データを暗号化するための疑似ランダムキーストリームを発生するためのアルゴリズムにおいて用いるための、元数を得るためにも用いられる、前記システム。

前記第１の出力値を含む前記桁の連続的に構成されたブロックが割り当てられる、前記システム内で用いるための出力パラメータは、移動局によって送信された通話された番号を隠蔽するために用いられる信号も含んでいる、前記システム。

１２．請求項１０記載のデジタルセルラ通信システムにおいて通信の機密性を強化するために用いられる複数のパラメータを発生するためのシステムにおいて、前記第１及び第２のアルゴリズムは、コードループの繰り返し実行をさんでいる、前記システム。

１３．請求項１０記載のデジタルセルラ通信システムにおいて通信の機密性を強化するために用いられる複数のパラメータを発生するためのシステムにおいて、前記入力信号及び前記キー桁は、バイトに集合化され、そして前記第１及び第２のアルゴリズムは、入力信号及びキー桁のバイトの夫々の対が繰り返し互いに加算される、混合過程を備えている、前記システム。

１４．請求項１０記載のデジタルセルラ通信システムにおいて通信の機密性を強化するために用いられる複数のパラメータを発生するためのシステムであって、

前記システムを各移動局のホーム交換に実施するための手段も備えている、前記システム。

１５．請求項１３記載のデジタルセルラ通信システムにおいて通信の機密性を強化するために用いられる複数の

明　細　書

デジタルセルラ通信用認証システム

関連出願に対する参照

本出願は、「デジタルセルラ通信用暗号化システム」と題された係属中の米国特許出願連番第５５６，３５８号、「セルラ通信システム用連続暗号同期」と題された係属中の米国特許出願第５５５，１０２号、及び「ハンドオフ時における暗号化システムの行動同期」と題された係属中の米国特許出願第５５６，１０３号に関連する主題を含んでおり、これらのあるものは１９９０年７月２０に出願され、本発明の譲受人に譲渡されたものである。このような出願及びその中の開示を、以下参照のためにここに組み入れることにする。

発明の背景

発明の分野

本発明はデジタルセルラ通信システムに関し、更に特定すれば、このようなシステムにおいてデータ通信の機密性を強化するための方法及び装置に関するものである。

従来技術の概要

セルラ無線通信は、恐らく、全世界の遠隔通信工業において最も急成長している分野である。セルラ無線通信システムは、現在稼動中の遠隔通信システムの小さな断片のみを含むものであるが、この断片は急激に増加し、そう遠くない将来において通信通信市場全体の大部分を代表するようになるだろうと、広く信じられている。この確信は、ネットワーク内の加入者と接続するために、主に配線技術に頼っている従来の電話通信ネットワークに固有な限界に、基づくものである。標準的家庭用または事務所用電話は、例えば、数の引き出し口即ち電話ジャックにある最大五の電話線を介して接続されている。周知に、電線が電話の引き出し口を、電話会社の区間内スイッチング事務所に接続している。したがって、電話ユーザの行動範囲は、電話線の長さだけでなく、動作可能な電話引き出しと、即ち区間内スイッチング事務所と接続された引き出し口の使用可能性によって、制限されることになる。実際、セルラ無線システムの発生は、これらの制限を克服し、電話ユーザに彼の効果的に他の人と通信する可能性を確性にすることなく、動き回ったり、または彼の家庭または事務所から移動する自由を与えるという希望に依るところが大きいのかもしれない。典型的なセルラ通信システムでは、ユーザ、またはユーザの車両が、比較的小さな無線装置を携帯し、これが基地局と通信し、そしてシステム内の他の移動局及び公衆切り換え式電話ネットワーク（ＰＳＴＮ）内の陸線網とユーザを接続する。

既存のセルラ無線通信システムの重大な不利は、アナログ無線伝送が容易され得る容易性である。特に、移動局と基地局との間の通信のいくらか或いは全ては、認証なしで、単に通信の単一または複数の周波数に適切な電子式受信機を同調させることによって、モニタすることができるのである。したがって、このような受信機へのアクセス及び鉄板に興味を有する者はだれでも、意思があれば、そして全く苦労なく、事実上通信のプライバシーを侵害することができてしまう。電子的盗聴を違法とする努力がなされて来たが、このような行動の秘匿性は、盗聴の全くではなくとも殆どが発見されずに起こるので、したがって動せられることも、引止められることもないことを意味する。ある競合者即ち敵が、ある人の直面上は個人的な電話での会話に「同調させる」ことを決心する可能性は、これまでセルラ無線通信システムの急増を妨げ、チェックされないままであり、このようなシステムの実害系及び政府での用途の育成力を弱かし続けるであろう。

最近、未来のセルラ無線通話通信システムが、アナログ技術よりむしろデジタルを用いて実施されるであろうことが称確になってきた。デジタルへの切り換えは、主として、システムの速度及び容量に関連する考慮によって、余じられたものである。単一のアナログ、または音声の無線周波数（ＲＦ）チャンネルは、４ないし６の、デジタルまたはデータの、ＲＦチャンネルを収容することができる。したがって、音声チャンネルを介して伝送する前に対話をデジタル化することによって、チャンネル容量、そして結果的にシステム全体の容量は、音声チャンネルの帯域を増加させることなく、劇的に増加され得るのである。自然の結果として、システムは、大幅に低いコストで、かなりのより大きな数の移動局を扱うことができる。

アナログからデジタルセルラ無線システムへの切り換えは、基地局と移動局との間の通信の機密性が欠如する可能性をいくらか改善するが、電子的盗聴の危険性は、相応からはかけ離れている。デジタル信号をデコードし、元の対話を発生できるデジタル受信機を構成することができるからである。アナログ伝送の場合より、ハードウエアはより複雑となり、手間はより高価となるだろうが、デジタルセルラ無線システムにおいて非常に個人的なまたは高度な価値さを要する会話が第三者によって傍受され、もしかすると用いられてシステムのユーザに損害を与え得る可能性が存続する。更に、電話の会話を第三者が盗聴する実際の可能性が、セルラ通話通信を規定の政府の通信手段としては、排除してしまうことになる。特定のビジネスユーザも同様に、機密性が欠如する可能性にさえも敏感であるかもしれない。したがって、セルラシステムを従来の電話ネットワークに実行可能な代替物とするためには、通信の機密性が少なくともいくつかの回路上で得られなければならない。

種々の解決法が、係留データの新線伝送によって生じる機密性の問題を軽減するために、提案されてきた。ある公知の解決法は、いくつかの既存の通信システムによ

って実施され、暗号アルゴリズム（ｃｒｙｐｔｏａｌｇｏｒｉｔｈｍ）を用いて、伝送に先立ってデジタルデータを理解不能な形状にスクランブルするものである。例えば、１９９０年６月付のリック　グレハン（Ｒｉｃｋ　Ｇｒｅｈａｎ）による雑誌バイト内の「クロック及びデータ」という題の論文の３１１－３２４ページは、暗号技システムの一般的な議論に関するものである。現在入手可能なシステムの殆どにおいて、スピーチは暗号化装置によってデジタル化されかつ処理されて、それが許可された受信機において暗号解読されるまで、事実上ランダム或いは疑似ランダムとなって現れる通信信号を生成する。暗号化装置によって用いられる特定のアルゴリズムは、独占的なアルゴリズムであることも、パブリックドメインにおいて見出されるアルゴリズムであることもある。このような技術に対するその性の背景が、１９７９年８月付のサイエンティフィックアメリカ（Ｓｃｉｅｎｔｉｆｉｃ　Ａｍｅｒｉｃａ）の１４８－１６７ページの、マーティン　Ｅ．ヘルマン（Ｍａｒｔｉｎ　Ｅ．Ｈｅｌｌｍａｎｎ）の「公開キーを用いる暗号性の数学」と題された論文にも、見出すことができる。

データの暗号化のための１つの技術は、暗号化されるデータと組み合わされる疑似ランダムビットのキーストリームを生成するものであり、「タイムオブデディ」または「フレーム番号」で駆動されるキーストリーム発生器に、頼ったものである。このようなキーストリーム発生器を、タイムオブデディカウンタ、即ち時間、分及びび、または単純な数カウンタに同期することができ、そして一方が他方との同期から外れた場合、送信機カウンタの現在のカウントを追従することによって、暗号化及び暗号解読装置を同期させることができる。　タイムオブデディまたはフレーム番号で駆動されるキーストリーム発生器を利用したシステムにおいて、通信の機密性を増加させるために、疑似ランダムキーストリーム内の各ビットの値を、暗号化キー内の全てのキービットの値の関数とすることが好ましい。このようにすると、暗号化された信号をデスクランブルしようとする人は、約５０から１００ビット或いはそれ以上かもしれない暗号化キーのビットの全てを「分解」即ち「解読」しなくてはならない。このタイプのキーストリームは、通常タイムオブデディカウンタのカウントを組み込んだ、選択されたアルゴリズムに応じて、数学的に暗号化キーワードを拡張することによって、生成される。しかしながら、暗号化キーの各ビットが全てのキーストリーム内の各ビットに影響を及ぼし、かつキーストリームが１つずつデータストリームビットに加えられるのであれば、１秒当たり必要なキーワード拡張計算の数は、膨大であり、システムのリアルタイム計算能力を容易に超過し得るものである。先に引用した、「デジタルセルラ通信用暗号化システム」と題された係属中の出願は、このようなキーストリームの記載を、従来のマイクロプロセッサの速度で、達成した。

暗号化キーを用いて、全てのキービットの複雑な関数である疑似ランダムキーストリームを発生するのは、デジタル通信の機密保持には非常に有用な手段である。他の手段には、各移動局に割り当てられた秘密のキー（永久キー）が、ホームネットワーク、即ち当該移動局の通常のサービス及び料金支払い領域の外側では、決して直接用いられないことを保証するための構成を含むこともできる。代わりに、特定の通話を暗号化するのに用いられた、ホームネットワークから訪問先ネットワーク、即ち移動局が動き回ったことがある通常の料金支払い領域以外の領域に、通信され得る他のビット（機密ビット）を発生するのに、上記永久キーを用が用いられる。このような構成は、水久的な秘密キーが第三者に解許可で開示されてしまい、そのキーを暗号化プロセスを乱破するために用いる危険性を減少するものである。

デジタルセルラシステム内の通信の機密を保つための更に別の手段は、登録時における移動局、通話の開始、または通話の受信の認証である。認証は、単に移動局の識別を確認するプロセスとして、見做されるかもしれない。認証と暗号化の双方は、訪問先ネットワークとホームネットワークとの間の通信を必要とし、ここで移動局は、暗号化に用いられる機密キーのような移動特定情報を得るために、水久的な登録を有している。本発明によれば、認証及び暗号化の機能を通信し、単一のネットワーク間やり取りが両方の機能を確立するようにしている。後に詳細に記載するように、本発明は、同一やり取りにおいて、ランダムな挑戦（ＲＡＮＤ）に対するキー依存応答（ＲＥＳＰ）だけでなく、ユーザトラフィックを暗号化するのに用いられる機密キー（Ｓ－キー）も発生することによって、このような統合を達成するものである。

現在開発中の米国デジタルセルラ（ＡＤＣ）システムでは、エアーインターフェースのみが、直接指定されている。しかしながら、ＡＤＣシステム内の所望の機密機能、例えば、認証及び暗号化の指定は、関係のにネットワークの機密性のアーキテクチャを決定し得るものである。認証に関しては、認証アルゴリズムがホームネットワークにおいて実行されるべきか、またはその代わりに訪問先ネットワークにおいて実行されるべきかに、アーキテクチャの取捨が係わってくる。ホームネットワークにおいて利用できるアルゴリズムへの可能な入力パラメータが、訪問先ネットワークにおいて利用できるそれらと同一である必要はないので、適切なアルゴリズムの定義のために、２つの取捨の間で選択が必要となる。後に説明するように、本発明は、ホームネットワークにおける認証アルゴリズムの実行に伴う、重要な機密性の喪失を考慮している。

既存のセルラシステムにおける重大な問題は、「不正移動局」症候群とも呼べるものである。これまで、ある

移動局のメモリ内容全体をコピーし、その情報を用いてネットワークからサービスを要求及び受信することができる複製物を製造することが可能であった。１つの提案された解決法は、各許可された移動局に、永久キーに対して書き込みのみのアクセスを有する、特定の認証モジュール、またはスマートカードを設けることである。この解決法は、しかしながら、移動局をより複雑かつより高価にしてしまう。本発明は、不正移動局の脅威に対して、より費用有効性が高い防護装置を提供する「ローリングキー」を考えている。加えて、ネットワークにおける「不正基地局」の脅威に応じるために、本発明は、ローリングキーを更新する時に用いられる、両方向性認証手順を備えている。この二方向認証手順は、機密性を高め、そして通信中いつでも、両方向認証をシステムの稼働中のトラフィックチャンネルにて実行できるようにするものである。各認証ステップは、ネットワーク操作者の随意で実行されるが、ある移動局の常在がネットワーク内で最初に検出された後には少なくとも１回実行されて、各初の通話に対してＳ－キーを発生するようにしなければならない。

移動局は時として、本発明の一般的システムに応じた認証及び暗号化を支援するのに必要とされるホームネットワークとの通信リンクを欠く、小さな孤立した訪問先ネットワーク内に入り込むことがある。このような訪問先ネットワークは、認証を実行せずに移動局からの通話または登録を受け入れ、そしてトラフィックチャンネル定義内の１ビットによって、移動局の移動識別等号（ＭＩＮ）がデフォルトＳ－キーとして用いられることを指示する選択を、行なうことができる。

本発明のシステムにつき、デジタルセルラシステム全体、及びセルラシステムにおいてトラフィックデータを暗号化するのに用いられる疑似ランダムキーストリームを発生するためのシステムに関して、以下に記載する。背景及びゴノまたは比較の目的で適切または有用な場合、ＥＩＡ／ＴＩＡ　暫定基準、「セルラシステムデュアルモード移動局－基地局の両立性の標準」ＩＳ－５４、１９９０年５月、電子工業会、ワシントンＤ．Ｃ．，Ｎ．Ｗ．，ペンシルバニア通り２００１，発行２０００号（以後「ＩＳ－５４」と呼び、その参照のためにここに載せる）を、参照する。

発明の概要

一観点において、本発明のシステムは、各移動局には唯一の多数桁秘密永久キーが割り当てられ、そして定期的に変化する多数桁ローリングキーが機密性を高めるために用いられている。デジタルセルラ通信システムにおける通信の機密性を強化するために用いられる複数のパラメータの発生を含んでいる。永久キーとローリングキーの両方は、各移動局と移動のホームネットワークに記憶されている。ある位置で、訪問先ネットワークからのランダム認証問い合せを表わす信号と、特定の移動局を表わす信号とを含む、複数の多数桁入力信号が、特定の移動局の多数桁永久キー及び特定の移動に関連した多数桁ローリングキーと共に、その特定の時刻に用いられる。

入力信号の桁が、第１の集合に構成され、入力信号のその集合と永久及びローリングキーの桁から、第１のアルゴリズムにしたがって、第１の出力値が計算される。前記第１の出力値を含む連続的に構成された桁のブロックが、訪問先ネットワークによる認証問い合せに対して返答するために移動局によって用いられる認証応答と移動局に対してそれを認証するために訪問先ネットワークによって用いられる認証信号とを含み、システム内で用いるための、選択されたパラメータに割り当てられる。次に入力信号の桁は第２の集合に構成され、入力信号のその集合と永久及びローリングキー桁から、第２のアルゴリズムにしたがって第２の出力値が計算される。前記第２の出力値を含む連続的に配列された桁のブロックが、システム内で通信データを暗号化するための疑似ランダムビットのキーストリームを計算するために用いられる機密キーと次の特定時刻において特定の移動と関連する新しいローリングキーとを含み、前記システム内で用いるための、選択されたパラメータに割り当てられる。

本発明の別の観点では、第１及び第２のアルゴリズムにおいて用いられる、あるランダム数が、参照テーブルから得られ、これも、システム内で通信データを暗号化するための疑似ランダムビットストリームを計算するためのアルゴリズムに用いられる、ランダム数を得るために用いられる。

本発明の更に別の観点では、両方向認証及び暗号化キー発生と共に、通信トラフィック暗号化を備えた、デジタルセルラ通信システムを実施するためのシステムが含まれる。

図面の簡単な説明

次の図面を参照することによって、本発明はよりよく理解され、その多数の目的及び利点は当業者には明白となろう。　第１図は、移動切り換えセンタ、複数の基地局及び複数の移動局を含む、セルラ無線通信システムの図式表現である。　第２図は、本発明のシステムの一実施例にしたがって用いられる移動局の装備の概略ブロック図である。

第３図は、本発明のシステムの一実施例にしたがって用いられる基地局の装備の概略ブロック図である。

第４図は、従来技術のキーストリーム発生器の概略ブロック図である。

第５図は、本発明にしたがって構成された暗号化システムのキーストリーム発生回路の概略ブロック図である。

第６図は、第５図に示されたキーストリーム発生器の第２拡張ステージの概略ブロック図である。

第７図は、厄知の標準による認証アルゴリズムの図式表現である。

第８図は、本発明による認証アルゴリズムの図式表現

である。

第９図は、本発明の認証アルゴリズム及び暗号化技術を用いた移動セルラシステムの図式表現である。

第１０図は、本発明の認証アルゴリズムにおいて用いられた混合過程の詳細ブロック図である。及び、

第１１図は、第１０図に示された混合プロセスの情報ブロックまたは混合セルの概略ブロック図である。

好適実施例の詳細な説明

デジタルセルラシステム

まず第１図を参照すると、そこには本発明が全体的に関係するタイプの、従来のセルラ無線通信システムが図示されている。第１図において、任意の地理的領域が、複数の連続無線通信範囲、即ちセルＣ１－Ｃ１０に分割されたものと、見ることができる。第１図のシステムは１０個のセルのみを含むものとして示されているが、実際にはセル数はそれより遥かに多いことは、明確に理解されよう。

セルＣ１－Ｃ１０のそれぞれ違いは、その中に配置されているのは、複数の基地局Ｂ１－Ｂ１０の対応する１つとして示された基地局である。基地局Ｂ１－Ｂ１０の各々は、当該技術においてよく知られているように、送信機、受信機及び制御器を備えている。第１図では、基地局Ｂ１－Ｂ１０は、先々セルＣ１－Ｃ１０の中央に配置され、全方向性アンテナを装備されている。しかしながら、セルラ無線システムの別の構成では、基地局Ｂ１－Ｂ１０は、間近近くに、またそうでなければ、セルＣ１－Ｃ１０の中央から離して配置されてもよく、全指向的または単一指向的にセルＣ１－Ｃ１０に無線信号を放すること が できる。したがって、第１図のセルラ無線システムの表現は、例示のみの目的のためのものであり、セルラ無線システムの可能な実施態様における利用として意図されたのではない。

第１図への参照を続けると、複数の移動局Ｍ１－Ｍ１０が、セルＣ１－Ｃ１０の中に見出されよう。再び、１０台の移動局のみが第１図に示されるが、実用では移動局の実際の数はそれよりかなり大きく、基地局の数を常に超過することが、理解されよう。更に、セルＣ１－Ｃ１０のいくつかには、移動局Ｍ１－Ｍ１０が見出されないが、移動局Ｍ１－Ｍ１０がセルＣ１－Ｃ１３のいずれか特定の１つに存在するかしないかは、１つのセル内のある位置から別の位置、或いは１つのセルから隣接または近くのセルに余儀する移動局Ｍ１－Ｍ１０の各々の個々の望みにしたがうものと、理解されよう。移動局Ｍ１－Ｍ１０の各々は、基地局Ｂ１－Ｂ１０の１つ以上、及び移動切り換えセンタＭＳＣを介して、電話通話を開始または受信することができる。移動切り換えセンタＭＳＣは、通信リンク、例えばケーブルによって、例示的な基地局Ｂ１－Ｂ１０の各々及び、図示しない固定公衆切り換え電話ネットワーク（ＰＳＴＮ）、または統合されたシステムデジタルネットワーク（ＩＳＤＮ）設備を備えた同様の固定ネットワークに接続されている。移動切り換えセンタＭＳＣと基地局Ｂ１－Ｂ１０との間、または移動切り換えセンタＭＳＣとＰＳＴＮまたはＩＳＤＮとの間の関連する接続は、第１図に完全には示されていないが、当業者にはよく知られたものである。同様に、セルラ無線システムには、１つ以上の移動切り換えセンタを備えていること、及び各々の追加した移動切り換えセンタを、異なるグループの基地局及び他の移動切り換えセンタに、ケーブルまたは無線リンクを介して、接続してあることも、公知である。

セルＣ１－Ｃ１０の各々を、複数の音声用もスピーチチャンネルと少なくとも１つのアクセスまたは制御チャンネルとに、割り当てる。制御チャンネルは、それらのユニットへ送信された及びから受信された情報によって、移動局の動作を制御または監督するために、用いられる。このような情報は、移動局が１つのセルの無線通用範囲外に、そして別のセルの無線通用範囲内に移動する際の、入来する通話信号、出立する通話信号、ページ信号、ページ応答信号、位置レイストレーション信号、音声チャンネル割り当て、保守指令、及び「ハンドオフ」指令を含むことができる。制御または音声チャンネルは、アナログまたはデジタルモード、またはそれらの組み合わせのいずれかで、動作することができる。デジタルモードでは、音声または制御信号のようなアナログメッセージは、ＲＦチャンネルを通じた送信の前に、デジタル信号表現に変換される。コンピュータによって poor いはデジタル化された音声装置によって発生されたもののような、純粋なデータメッセージは、デジタルチャンネルを通じて直接フォーマット及び送信してもよい。

時分割多重（ＴＤＭ）を用いているセルラ無線システムでは、複数のデジタルチャンネルが、共通のＲＦチャンネルを共有することができる。ＲＦチャンネルは、一連の「タイムスロット」に分割され、各々異なるデータ部からの情報のバーストを含み、かつガードタイムによって互いに分離されており、更にタイムスロットは、当該技術ではよく知られているように、「フレーム」にグループ化されている。フレーム当たりのタイムスロットの数は、ＲＦチャンネルによって収容されるよう試みられたデジタルチャンネルの帯域に依存して変化する。フレームは、例えば三（３）つのタイムスロットから成り、各々１つのデジタルチャンネルに割り当てられる。ここで論じられる本発明の一実施例では、１フレームは、３つのタイムスロットを含むように、指定されている。しかしながら、本発明の教示は、フレーム当たりいかなる数のタイムスロットを利用しているセルラ無線システムにでも、同等に応用可能であることが、明確に理解されよう。

移動局

次に第２図を参照すると、そこには、本発明の一実施

例にしたがって使用される移動局の装置の概略ブロック図が示されている。第２図に例示されている装置は、デジタルチャンネルを通じた通信用に、用いられるものである。マイクロフォン１００によって検出され、移動局による通信用に用いられる音声信号は、入力として、スピーチコーダ１０１に与えられ、これがアナログ音声信号をデジタルデータビットストリームに変換する。データビットストリームは、次に、デジタル通信の時分割多重アクセス（ＴＤＭＡ）技術にしたがって、データパケット即ちメッセージに分割される。高速関連制御チャンネル（ＦＡＣＣＨ）発生器１０２は、制御または監督メッセージを、セルラ無線システム内の基地局と交換する。従来のＦＡＣＣＨ発生器は、「ブランクアンドバースト（ｂｌａｎｋ ａｎｄ ｂｕｒｓｔ）」状に動作し、これによって、ユーザフレームのデータが無音化され、ＦＡＣＣＨ発生器１０２によって発生された制御メッセージが高速度で送信される。

ＦＡＣＣＨ発生器１０２のブランクアンドバースト動作とは対照的に、低速関連制御チャンネル（ＳＡＣＣＨ）発生器１０３は、連続的に制御メッセージを基地局と交換する。ＳＡＣＣＨ発生器の出力は、固定バイト長、例えば、１２ビットを割り当てられ、そしてメッセージ列（フレーム）内に各タイムスロットの一部として含まれる。チャンネルコーダ１０４、１０５、１０６は、スピーチコーダ１０１、ＦＡＣＣＨ発生器１０２及びＳＡＣＣＨ発生器１０３に、夫々接続されている。チャンネルコーダ１０４、１０５、１０６の各々は、スピーチコード内の重要なデータビットを保護する畳み込みエンコーディングの技術と、７ビットのエラーチェックを計算するために、スピーチコーダフレーム内の最上位ビット、例えば１２ビットが用いられる巡回冗長チェック（ＣＲＣ）を用いて入来データを操作することによって、エラー検出及び訂復を行なう。

再び第２図を参照して、チャンネルコーダ１０４、１０５は、デジタル化した音声メッセージの、ＦＡＣＣＨ監督メッセージとの時分割多重化のために用いられる、マルチプレクサ１０７の出力は、２－バーストインターリーバに結合されており、これが、移動局によって送信されるをデータメッセージ（例えば、２６０ビットを含むメッセージ）を、２つの連続タイムスロットに配置された２つの同等であるが別個の部分（各部分は１３０ビットを含む）に分割する。このようにして、レイリー（Ｒａｙｌｅｉｇｈ）フェーディングの劣化効果を大幅に減少させることができる。２－バーストインターリーバ１０８の出力は、入力として、モジュロ－２加算器１０９に与えられ、ここで、送信すべきデータは、以下に記載する本発明のシステムにしたがって発生される、疑似ランダムキーストリームとの論理的モジュロ－２の加算によって、ビット毎に暗号化される。　チャンネルコーダ１０６の出力は、入力として、２２－バーストインターリーバ１１０に与えられる。２２－バーストインターリーバ１１０は、ＳＡＣＣＨデータを、２２個の連続タイムスロットに分割するが、各々は１２バイトの制御情報から成る１バイトによって占められている。インターリーブされたＳＡＣＣＨデータは、バースト発生器１１１への入力の１つを形成する。バースト発生器１１１への別の入力は、モジュロ－２加算器１０９の出力によって与えられる。バースト発生器１１１は、データの「メッセージバースト」を生成するが、各々は、以下に更に説明するように、タイムスロット識別子（ＴＩ）、デジタル音声カラーコード（ＤＶＣＣ）、制御または監督情報、及び送信すべきデータを含んでいる。

１フレーム中のタイムスロットの各々にて送信されるのは、タイムスロットの識別及び受信機の同期に用いられるタイムスロット識別子（ＴＩ）と、連切なチャンネルがデコードされていることを保証するデジタル音声カラーコード（ＤＶＣＣ）である。本発明のフレーム例では、１組の３つの異なる２８ビットのＴＩが、各タイムスロットに対して１つ定義され、一方、同一の８ビットＤＶＣＣが３つのタイムスロットの各々の中で送信される。ＴＩ及びＤＶＣＣは、第２図に示すように、バースト発生器１１１に接続された同期器／ＤＶＣＣ発生器１１２によって、移動局内に与えられる。バースト発生器１１１は、モジュロ－２加算器１０９、２２－バーストインターリーバ１１０及び同期器／ＤＶＣＣ発生器１１２の出力を組み合わせて、各々データ（２６０ビット）、ＳＡＣＣＨ情報（１２ビット）、ＴＩ（２６ビット）、コード化されたＤＶＣＣ（１２ビット）、及びＥＩＡ／ＴＩＡ　ＩＳ－５４によって指定されたタイムスロットフォーマットにしたがって統合された合計３２４ビットに対する１２０区切りビットから成る、一連のメッセージバーストを発生する。

メッセージバーストの各々は、先に論じたように、１つのフレームに含まれる３つのタイムスロットの１つの中で送信される。バースト発生器１１１は、イコライザ１１３に接続され、これは１つのタイムスロットの送信を、他の２つのタイムスロットの送信と同期させるのに必要なタイミングを与える。イコライザ１１３は、基地局（マスタ）から移動局（スレーブ）に送られるタイミング信号を検出し、それによって－バースト発生器１１１を同期させる。イコライザ１１３は、ＴＩ及びＤＶＣＣの値をチェックするために用いることもできる。バースト発生器１１１は、２０ｍｓのフレームカウンタ１１４にも接続されており、これは、２０ｍｓ毎、即ち送信されるフレーム毎に、移動局によって附加される暗号化コードを更新するのに用いられる。暗号化コードは、数学アルゴリズムを用い、各移動局に対して唯一であるキー１１５の制御の下に、暗号化ユニット１１５によって発生される。このアルゴリズムは、本発明にしたがって、

そして更に以下に論ずるように、疑似ランダムキーストリームを発生するのに用いることができる。

バースト発生器１１０によって生成されたメッセージバーストは、ＲＦ変調器１１７に、入力として与えられる。ＲＦ変調器１１７は、／４－ＤＱＰＳＫ技術（／４シフトされた、差動的エンコード直角位相シフトキー）にしたがって、搬送波周波数を変調するために用いられる。この技術の使用は、移動局によって送信される情報は、差動的にエンコードされる、即ち、２つのビットシンボルが、位相の４つの可能性のある変化、＋または－　／４　及び＋または－　３／３、として、送信されることを暗示している。選択された送信チャンネルに対する搬送波周波数は、送信周波数合成器１１８によって、ＲＦ変調器１１７に供給される。ＲＦ変調器１１７のバースト変調された搬送波信号出力は、出力増幅器１１９によって増幅され、そしてアンテナ１２０を介して、基地局に送信される。

移動局は、受信機１２２に接続されているアンテナ１２１を介して、基地局からのバースト変調された信号を受信する。選択された受信チャンネルに対する受信機搬送波周波数は、受信周波数合成器１２３によって発生され、ＲＦ復調器１２４に供給される。ＲＦ復調器１２４は、受信した搬送波信号を中間周波数信号に復調するのに用いられる。この中間周波数信号を、更にＩＦ復調器１２５によって復調し、／４－ＤＱＰＳＫ変調の前に存在していたような元のデジタル情報を復元する。このデジタル情報は、次にイコライザ１１３を通って、シンボル検出器１２６に達し、イコライザ１１４によって与えられたデジタルデータの２－ビットシンボルフォーマットを、単一ビットのデータストリームに変換する。

シンボル検出器１２６は、２つの別個の出力、即ち、デジタル化されたスピーチデータとＦＡＣＣＨデータとから成る第１の出力と、ＳＡＣＣＨデータから成る第２の出力とを、生成する。第１の出力は、２－バーストデインターリーバ１２８に接続されているモジュロー２加算器１２７に供給される。モジュロー２加算器１２７は、暗号化ユニット１１５に接続されており、データを暗号化するために基地局内の送信機によって用いられ、かつ以下に記載する本発明の教示にしたがって発生されたのと同一の疑似ランダムキーストリームを、ビット毎に、減算することによって、４つの暗号化され送信されたデータを暗号解読するのに用いられる。モジュロー２加算器１２７及び２－バーストデインターリーバ１２８は、２つの連続したフレームのデジタルデータから得られた情報を組み立てそして再構成することによって、スピーチ／ＦＡＣＣＨデータを再構築する。２－バーストデインターリーバ１２８は、２つのチャンネルデコーダ１２９、１３０に結合されており、これらはコード化と逆の過程を用いて畳み込み状にエンコードされたスピーチ／ＦＡＣＣＨデータをデコードし、サイクリックリダンダンシチェック（ＣＲＣ）ビットをチェックして、エラーが発生していないか判断する。チャンネルデコーダ１２９、１３０は、一方でスピーチデータ、そして他方でいずれかのＦＡＣＣＨデータ間の相違を検出し、スピーチデータ及びＦＡＣＣＨデータを、スピーチ検出器１３１及びＦＡＣＣＨ検出器１３２に、夫々差し向ける。スピーチ検出器１３１は、チャンネルデコーダ１２９によって供給されたスピーチデータを、スピーチコーダアルゴリズム、例えばＶＳＥＬＰにしたがって処理し、そして基地局によって送信され移動局によって受信されたスピーチ信号を表わすアナログ信号を発生する。次に、フィルタ処理技術を用いて、スピーカ１３３による同報通信に先立って、前記アナログ信号の品質を高めることもできる。ＦＡＣＣＨ検出器１３２によって検出されたいかなるＦＡＣＣＨメッセージも、マイクロプロセッサ１３４に送られる。

シンボル検出器１２６の第２の出力（ＳＡＣＣＨデータ）は、２２－バーストデインターリーバ１３５に供給される。２２－バーストデインターリーバ１３５は、２２の連続フレームにわたって広げられたＳＡＣＣＨデータの再組み立て及び再構成を行なう。２２－バーストデインターリーバ１３５の出力は、入力として、チャンネル検出器１３６に与えられる。ＦＡＣＣＨメッセージは、ＳＡＣＣＨ検出器１３７によって検出され、制御情報がマイクロプロセッサ１３４に転送される。

マイクロプロセッサ１３４は、移動局の活動、及び移動局と基地局との間の通信を制御するものである。基地局から受信したメッセージにしたがって、マイクロプロセッサ１３４によって決定が行なわれ、そして移動局によって測定が行なわれる。マイクロプロセッサ１３４は、端末キーボード入力及び表示出力ユニット１３８も、備えている。キーボード及び表示ユニット１３８は、移動局のユーザが、基地局と情報を交換できるようにするものである。

基地局

次に、第３図を参照すると、本発明にしたがって用いられる基地局の装備の概略ブロック図が示されている。第２図に示された移動局の装備を、第３図に示された基地局機器と比較すると、移動局及び基地局によって用いられている装備の多くは、構造及び機能において、実質的に同一であることが、示される。このような同一の装備は、便宜上そして一貫性のために、第２図に関連して用いたものと同一の参照番号を第３図に付番するが、第３図ではダッシュ（'）を付加えることによって、区別することにする。

しかしながら、移動局と基地局装備との間には幾らかの細かい相違がある。例えば、基地局は、１本のみではなく、２本の受信アンテナ１２１'を有する。受信アンテナ１２１'の各々に関連するのは、受信機１２２'、ＲＦ復調器１２４'、そしてＩＦ復調器１２５'である。

更に、基地局は、プログラマブル周波数組み合わせ器（ｃｏｍｂｉｎｅｒ）１１８Ａ’を備えており、これは送信周波数合成器１１８’に接続されている。周波数組み合わせ器１１８Ａ’と送信周波数合成器１１８’は、適用可能なセルラ周波数再使用計画にしたがって、基地局によって用いられるＲＦチャンネルの選択を遂行する。基地局は、しかしながら、移動局にあるユーザキーボード及び表示ユニット１３８に類似したユーザキーボード及び表示ユニットを備えていない。しかし、これは、２つの受信機１２２’の各々から受信した信号を測定するため、そして、マイクロプロセッサ１３４’に出力を与えるために接続された信号レベルメータ１００’を備えている。移動局と基地局との間の装備におけるその他の相違も存在するが、それは当該技術ではよく知られたものである。

これまでの議論は、本発明のシステムの動作環境に焦点を当てたものであった。以下、本発明の特定実施例の具体的な説明を記載する。先に開示し、以後用いられるように、「キーストリーム」という用語は、例えば、ＲＦチャンネルのような、送信または媒体への配信に先立ってデジタル的にエンコードされた、権許可のアクセスを受けやすい、メッセージまたはデータ信号を暗号化するのに用いられる疑似ランダムな一連の二進ビットまたはビットブロックを意味する。「キーストリーム発生器」は、複数のビットから成る秘密キーを処理することによって、キーストリームを発生する装置を意味する。暗号化は、単に、キーストリームの暗号化されるデータへのモジュロ－２加算によって、実行することができる。同様に、暗号解読は、暗号化されたデータからのキーストリームの同一コピーのモジュロ－２減算によって実行される。

キーストリームの発生

総じて言えば、キーストリーム発生器は、大々第２及び第３図の要素１１５及び１１５’によって置われる、比較的小数の秘密ビット、即ち要素１１８及び１１８’で表わされる秘密キーを、送信（または配信）に先立ってデータメッセージを暗号化するのに用いられる、かなり大きな数のキーストリームビットに拡張する機構を提供するものである。エンコードされたメッセージを暗号解読するには、受信機は、そのメッセージを暗号化するのに用いられたキーストリームビットへのインデックスを「知って」いなければならない。言い換えれば、受信機は、同一キーストリーム発生器を有し送信機と同一キーストリームビットを生成するのみならず、メッセージを適切にデコードする場合、受信機のキーストリーム発生器を送信機のキーストリーム発生器と同期して動作させなければならない。通常、同期は、キーストリームビットの発生に参加したビット、ブロックまたはメッセージカウンタのような、内部メモリ素子等の内容を、エンコーディングシステムからデコーディングシステムまで定期的に通信することによって、達成される。しかしながら、同期は、二進カウンタのような事前的ビットブロックカウンタを用い、キーストリームビットの新しいブロックが生成される毎にそれらのカウンタをある量だけ増分することにより、明示化することができる。このようなカウンタは、リアルタイム、即ち、時間、分、秒、のクロックチェーンの一部を形成することができる。後者の形式のカウンタに関するキーストリーム発生器は、先に引用した、「タイムオブデイ」駆動型キーストリーム発生器として知られている。

キーストリーム発生器のビット毎またはブロック毎の前進（ａｄｖａｎｃｉｎｇ）に用いられる正確な方法、及び送信回路や受信回路と同期させるのに用いられる特定の方法は、上述のように、「セルラ通信システム用適応暗号同期」と題された係属中の特許出願通事第＿＿＿＿号の主題であることに注意されたい。本発明のシステムは、以後詳細に述べるように、例えば、セルラ通信通信システムにおけるＲＦチャンネルを選じたデジタル通話を防護するのに用いることができる、効果的な暗号化システムの有効な実施に向けられたものである。この暗号化システムは、秘密キーに含まれている複数のキービットに対して、幾何多数のブール演算を行なうことにより、かなりの数のキーストリームビットを生成する、キーストリーム発生器を備えている。本発明のキーストリーム発生器は、開示なマイクロプロセッサアーキテクチャを有する典型回路を用いて、実施することができる。

次に第４図を参照すると、従来技術のキーストリーム発生器の概略ブロック図をここで見ることができる。適応的なブロックカウンタ２０１は、組み合わせ論理回路２０２への第１の多ビット入力を与える。複数のＩビットメモリ素子、即ちフリップフロップｍ１、ｍ２、ｍ３、．．．ｍｎが、組み合わせ論理回路への第２の多ビット入力を与える。Ｉビットの出力ｄ１、ｄ２、ｄ３．．．、ｄｎから成る組み合わせ論理回路２０２の出力の一部は、フリップフロップｍ１－ｍｎにフィードバックされる。フリップフロップｍ１－ｍｎに供給されるこれら一連のビットクロック入力パルス内の各クロックパルスの後に、出力ｄ１－ｄｎは夫々フリップフロップｍ１－ｍｎの次の状態となる。組み合わせ論理回路２０２の相応しい構造によって、ストレート二進カウンタ、最大長シーケンスを実行する線形フィードバックシフトレジスタ、またはその他のいずれかの形式の線形または非線形最適カウンタを形成するようにし、フリップフロップｍ１－ｍｎを構成することができる。いずれの場合でも、受信機構における各フリップフロップｍ１－ｍｎの状態の各々、及びブロックカウンタの状態は、送信機構における対応する要素の状態と同一としなければならない。リセットまたは同期機構２０４が、受信機を送信機と同期させるのに用いられる。

第４図への参照を続けて、複数の秘密キービットｋ１、

ｋ２、ｋ３．．．ｋｎは、組み合わせ論理回路２０２への第３の多ビット入力を形成している。秘密キービットの数ｓは、常に１００ビットプラスまたはマイナス（＋／－）２の冪の領域にある。秘密キーｋ１－ｋｎの各々が、少なくとも、キーストリーム内のビットの各々に影響を及ぼす可能性を有することが望ましい。そうでないと、盗聴する場合、暗号化されたデータを暗号解読しモニタするために、秘密キービットｋ１－ｋｎの値かサブセットのみを解読すればよいことになる。不許可の侵受の危険性は、しかしながら、キーストリーム内の各ビットの値（論理状態）を、特定の秘密キービットの値だけでなく、全ての他の秘密キービットの値、並びにブロックカウンタ２０１の状態及び他の内部メモリ状態にも依存させるようにすれば、大幅に減少させることができる。これまで、このような依存性の確立は、歩外な数のブール演算を伴うものであった。例えば、秘密キーが、１００個の秘密キービットから成るものと仮定する。これら秘密キービットの各々がキーストリーム内の各ビットに影響を与えると、キーストリーム内ビット当たり合計で１００個の組み合わせ演算が必要となろう。したがって、１万個のキーストリームビットを生成するには、合計で１００万個の組み合わせ演算が必要となり、更に各キーストリームビットを１つ以上の内部メモリ状態にも依存させるとすると、その数は更に大きなものとなろう。本発明の目的の１つは、各キーストリームビットの秘密キービットの各々による依存性を維持しつつ、キーストリームビット毎に必要とされる組み合わせ演算の数を大幅に減少させることである。

例えば、５０から１００個の秘密キービットからの、数千個の疑似ランダムなキーストリームビットの生成を、多段拡張過程として、見ることができる。複数の拡張ステージが共に縦属されており、各々が連続的により小さくなる拡張比を有している。最初のステージによる拡張は、キーストリームビット当たり必要な論理（ブール）演算数を最小化するために、後続のステージによるものより、少ない精度で実行される。加えて、最初の拡張ステージは、秘密キービットに対する依存性が高い確率の出力ビットを与えるように構成されており、後続のステージで実行されなければならない論理演算数を更に減少させている。

次に第５図を参照すると、キーストリーム発生器システムの最終ブロック図が示されている。複数の機密キービットｋ１、ｋ２、ｋ３．．．が、入力として第１ステージの拡張２０５に与えられる。機密キービットは、以下に更に詳しく記載する認証アルゴリズムによって、永久キービットから得ることができる。機密キービットｋ１、ｋ２、ｋ３．．．入力は、機密キービットｋ１、ｋ２、ｋ３．．．ｋｎの数つか、しかし好ましくは全てを含むことをもって、これを以後時々「秘密」キービットと呼ぶことにする。加えて、または随意的に、第１ステージの拡張２０５への入力は、メッセージカウンタの出力、ブロックカウンタ、フレーム開始時の時間またはブロックカウント数を表わすデートータイムスタンプ、または送り手及び受け手によって同期され得るその他の可変出力を、含むことができる。時間と共にゆっくりと変化するいかなる内部メモリ出力でも、第１ステージの拡張２０５への入力として、用いることができる。第１ステージの拡張２０５は、好たまま、例えばメッセージ毎に１回、変化されなければならないので、ゆっくりと変化する入力が望ましい。　第１ステージの拡張２０５は、秘密キービットｋ１、ｋ２、ｋ３．．．の数より、大幅に大きなサイズの拡張された出力を発生する。この拡張されたた出力は、メモリ素子２０６内に記憶され、組み合わせ論理回路２０７によってアクセスされる。組み合わせ論理２０７は、以下に更に完全に記載するような、第２ステージの拡張を行なうものである。カウンタ即ちレジスタ２０８の出力は、組み合わせ論理２０７への入力を形成する。レジスタ２０８は、キーストリームビットの各ブロックの発生に先立ち、新しい開始状態に初期化される。初期値発生器２０９は、レジスタ２０８にその開始状態を与える。この開始状態は、キーストリームビットの各特定ブロックに対して異なるが、当該特定ブロックのブロック数の関数であり、そして、秘密キービットｋ１－ｋｎのあるサブセットの関数ともすることができる。

組み合わせ論理２０７の第１の出力２１０は、レジスタ２０８にフィードバックされる。出力２１０は、演算の各サイクル後に、レジスタ２０８の新しい状態となる。組み合わせ論理２０７の第２の出力２１１は、先の第２及び３図に示したように、データストリームと関連されることになるキーストリームビットを形成する。出力２１１においてサイクル毎に生成されるキーストリームビットの数は、いずれかの２の冪数、即ち、８、１６、３２、５６等とすることができる。このようなビットを、まとめて「キーワード」と呼ぶことにする。レジスタ２０８の再初期化の前に出力２１１において生成されたキーワードのいくつかまたは全ては、キーブロック２１２にグループ化される。キーブロック２１２は、例えば、レジスタ２０８の再初期化に先立って、サイクル毎または１サイクルおきに生成される全てのキーワードから成るものである。

第５図に描かれそして先に論じたキーストリーム発生器システムの従来の実施は、多数の複雑な組み合わせ論理回路が必要であり、これは複数の論理ゲート、即ちアンド（ＡＮＤ）、オア（ＯＲ）等を相互接続することによって回路に実現されたとすると、非常に特定された用途にのみ有用な、巨大で高価なチップとなることを、当業者であれば認めるであろう。一方、算術及び論理ユニット（ＡＬＵ）は、種々の小型、低価格、そして多目的マイクロプロセッサの原型構成物である。本発明は、このようなＡＬＵを用いて、必要な組み合わせ論理機能の

全てを実現するための手段を提供するものである。

次来のＡＬＵは、プログラムの制御下で動作し、いずれか２つの８ビットまたは１６ビット二進語間で、組み合わせ関数ＡＤＤ、ＳＵＢＴＲＡＣＴ、ＢＩＴＷＩＳＥ ＥＸＣＬＵＳＩＶＥ ＯＲ、ＡＮＤ、ＣＲを実行することができる。ＡＬＵが、第５図の装置において必要とされるプール関数の全てを連続的に実施するのに用いられる場合、実行され得る１秒毎の完全サイクル数に関して測定されたＡＬＵ動作速度は、大幅に減少されていよう。本システムにおいて用いられる多段試験は、しかしながら、最も頻繁に実行される組み合わせ論理２０７から第１ステージの拡張２０５における大量のキー依存関数の結果でない定期的な計算までに対して、サイクル当たりのプログラム命令数、即ちＡＬＵを利用する回数を最小化することによって、ＡＬＵ速度の過度の減少を防止する。先の文における単語「大きな」によって、例えば、秘密キービット数ｎより大きな程度の等級が要求される。 一旦レジスタ２０８が開始値で初期化されると、組み合わせ論理２０７は、出力２１１にキーワードのストリームを発生し、そしてレジスタ２０８がフィードバック値を出力２１０において再びロードされる毎に、追加キーワードを発生し続ける。しかしながら、キーワード発生過程の保全性を密かに損い得る問題が生じることがある。例えば、レジスタ２０８の内容が常にそれらの初期値に戻るとすると、これまでに発生されたキーワードが再び繰り返されることになる。同様に、レジスタ２０８の内容が、現在のキーブロックの発生において既に見出された値（初期値である必要はない）に戻ると、システムは、「短縮サイクル」を行なっていると言われる。以前に示唆した理由、例えば、不許可の暗号解読の容易さのため、単一のキーブロックの発生において、キーワードの連続的繰り返し始まること、または短縮サイクルが起こることは、望ましいことではない。更に、レジスタ２０８の内容が、ある点、例えばＭ番目のキーワードを発生した後に、別のキーブロックの発生後に存在した或いは存在するであろううちの値と等しくなると、２つのキーブロックは、その点以降、同一となり、これも望ましくない出来事である。 したがって、組み合わせ論理２０７と関連するレジスタ２０８（「組み合わせ論理／レジスタの組み合わせ」）は、ある回数連続的に動作する時、（１）ブロック当たりのキーワード数より短いサイクルを生成するのではなく、そして（１１）レジスタ２０８の唯一の開始状態毎に唯一のキーワード列を生成するべきである。後者の要件を満たすためには、２つの異なる開始状態が、同一状態に収束できないようにすればよい。更に、前述の要件の両方は、メモリ２０８の内容には関係無く適用されればよい。以下により詳細に説明するように、本発明はこれらの問題を軽減し、そしてキーワード発生過程の保全性を強化するものである。

組み合わせ論理／レジスタの組み合わせの状態遷移図が収束する分岐点を有する時、そのような組み合わせは、どちらの道を取るかについての曖昧さのため、このような分岐点を介して逆に実行することはできない。したがって、組み合わせを処理する過程が曖昧でないこと、または逆可能であることが示されれば、収束分岐点はその状態遷移図には存在しないことの証明となる。このような過程を以下に記載し、かつ論じることにする。

次に第３図を参照すると、第５図に示したキーストリーム発生器の第２拡張ステージの部分的概略ブロック図が、ここに見られる。第５図のレジスタ２０８は、第６図では３つのバイト長レジスタ２０８Ａ、２０８Ｂ、２０８Ｃに分割されている。レジスタ２０８Ａ、２０８Ｂ、２０８Ｃは、例えば、８ビットレジスタとすることができる。レジスタ２０８Ａ、２０８Ｂ、２０８Ｃの初期化に続いて、新しい状態値が、次の式から計算される。

（１） Ａ′＝Ａ＃［Ｋ（Ｂ）＋Ｋ（Ｃ）］

（２） Ｂ′＝Ｂ＃Ｒ（Ａ）

（３） Ｃ′＝Ｃ＋１

ここで、

Ａ′は、レジスタ２０８Ａに対する新しい状態値であり、Ｂ′は、レジスタ２０８Ｂに対する新しい状態値であり、Ｃ′は、レジスタ２０８Ｃに対する新しい状態値であり、Ａは、レジスタ２０８Ａに対する現在の状態値であり、Ｂは、レジスタ２０８Ｂに対する現在の状態値であり、Ｃは、レジスタ２０８Ｃに対する現在の状態値であり、＋は、ワード長モジュロ加算、例えば、バイト幅モジュロ－２５６の加算を意味し、

＃は、＋（上で定義したように）または、ビットワイズ（ｂｉｔｗｉｓｅ）の排他的オア（ＸＯＲ）を意味し、

Ｋ（Ｂ）は、第５図に示したメモリ２０５のアドレスＢに配置された値Ｋであり、

Ｋ（Ｃ）は、第５図に示したメモリ２０５のアドレスＣに配置された値Ｋである。

メモリ２０６に配置された値Ｒの各＋は、第５図に示す第１ステージの拡張２０５によって、既に計算され、全ての秘密キーセットの複雑な関数となったことに、注意されたい。Ｒ（Ａ）は、既証アルゴリズムに用いられるＳ－ボックスの内容に関して以下に説明するその同一のテーブル（ｔａｂｌｅ）である、固定参照テーブルＲ内のアドレスＡに配置された値である。また、Ａのビットは、入力として、出力Ｒを生成する組み合わせ論理ブロックに供給される。参照テーブルＲ、またはその代わりに、組み合わせ論理ブロックは、Ａのワード長以上で、Ｂのワード長以下の数の出力ビットを与えるなければならない。Ａ及びＢが両方共８ビットバイトである場合、例えば、Ｒも８ビットバイトで、参照テーブルＲは２５６個の値を含むことになる。

値Ｒは、入力から出力に１：１のマッピングを育せねばならない。即ち、入力ビットの各可能性のある状態は、唯一の出力値に割り付けなければならない。これは、Ｒ

関数が逆転可能であることを保証し、これが更に、全通程を、以下における関係によって、逆転できることを保証するものである。　（１）Ｃ＝Ｃ－１

（２）Ｂ＝Ｂ＃＃Ｒ’（Ａ）

（３）Ａ＝Ａ＃＃［Ｋ（Ｂ）＋Ｋ（Ｃ）］

ここで、

－は、ワード長のモジュロ減算を意味し、

＃＃は、＃の逆演算、即ち、－（先に定義したような）またはビットワイズＸＯＲを、意味し、及び

Ｒ’は、１：１参照テーブル、または組み合わせ論理Ｒの逆である。

この逆転可能性は、上述の組み合わせ論理／レジスタの組み合わせの状態遷移図には収束分岐点がないことを示しており、したがって、全ての開始状態が唯一のキーワード列を発生することを保証している。更に、Ｃが１ずつのみ増分され、そして２Ｗ回の繰り返しの後までその初期値には戻らないので（Ｗは用いたワード長）、この通程は、最小サイクル長を保証するものである。例えば、皆Ａ、Ｂ、Ｃ、Ｒ及びＫの全てが８ビットバイトの場合、最小サイクル長は２５６となる。各繰り返し（サイクル）毎に、１つのキーワード（バイト）が抽出されると、列の中途半端な繰り返しの恐れがなく、合計２５６バイトを抽出することができる。一方、２度の繰り返し毎に１回キーワードが抽出されると、列の中途半端な繰り返しなしに、合計１２８個のキーワードを抽出することができる。前の２つの文における単語「抽出」によって、キーワードの収集と、第５図におけるキーブロック２１２のようなキーブロックへの配置を、意味する。本発明に用いることができるキーワード抽出の特定の方法を、すぐ後に述べる。

第６図に関して、レジスタ２０８にフィードバックされる、組み合わせ論理２０７の出力２１０を計算するための通程を述べた。一般的に言うと、中間量Ａ、Ｂまたはこのいずれか１つを、直接抽出し、各繰り返しにおいてキーワードとして用いることもできる。Ｓ＝（Ａ、Ｂ、Ｃ）が組み合わせ論理／レジスタの組み合わせの現在の状態を表わすとすると、Ｓ０への初期化に続いて、一連の状態Ｓ０、Ｓ１、Ｓ２、Ｓ３、Ｓ４、Ｓ５、Ｓ６、Ｓ７．．．というように遷移することになろう。しかしながら、後続のキーブロックの計算において、レジスタが例えばＳ２に初期化されると、その結果の列Ｓ２、Ｓ３、Ｓ４、Ｓ５、Ｓ６、Ｓ７．．．は、２つのキーワード（Ｓ０、Ｓ１）だけシフトした最初の列と同一となる。したがって、状態Ｓからの個人、Ｂ、Ｃが直接キーワードとして用いられると、このような同一性が異なるキーブロック間で表われるかもしれない。これを防止するために、本発明のシステムは、キーブロック内の組の位置にしたがって抽出された個の各々を変更して、同一個が別のブロック内の異なるキーワード位置に抽出された場合、異なるキーワードが得られるようにしている。換言することができる。

Ｎを現計算中のキーブロック内のキーワードの数とし、Ｓ＝（Ａ、Ｂ、Ｃ）をキーワードＮが抽出されようとする繰り返しにおけるレジスタ２０８の現在の状態とする。キーワードＷ（Ｎ）の組は、次のように計算することができる。

Ｗ（Ｎ）＝Ｂ　＋’　Ｋ［Ａ＋Ｎ］

ここで、

＋は、ＸＯＲを意味し、

＋’は、＋（直前で定義した）またはワード長－モジュロ加算のいずれかを意味する。

キーワード抽出のための他の相応しい例示的方法は、次を含んでもよい。

Ｗ（Ｎ）　＝　Ｂ　＋　Ｋ［Ｒ（Ａ＋Ｎ）］または

Ｗ（Ｎ）　＝　Ｒ［Ａ＋Ｎ］＋Ｋ［Ｂ＋Ｎ］等。

システムにおいて最良の暗号法の特性を得るには、抽出されたキーワードの個が、キーブロック内におけるそれらの夫々の位置の関数となることを、推奨する。

データの暗号化に用いられる、多数の複雑なキー依存疑似ランダム（ＰＲ）ビットを発生し、かつ従来のマイクロプロセッサに実施され得る、暗号化システムを説明したが、暗号化と認証機能を統合し、デジタルセルラシステムの全体の機密性を改善するシステムの説明を、すぐ下に記載する。

認証

本発明による認証の通程は、一般的に次の一連のステップを含んでいる。

（１）移動局は、移動識別番号（ＭＩＮ）を暗号化されていない形式で送ることによって、それ自身をネットワークに対して識別し、ネットワークが、その移動に関する情報、例えば機密キーを、それらが記憶されている場所またはデータベースから、検索できるようにしている。

（２）ネットワークはランダム挑戦個号（ＲＡＮＤ）を移動に通信する。

（３）移動局及びネットワークは、ある公開したアルゴリズム（以後ＡＵＴＨ１と呼ぶ）にしたがって、ＲＡＮＤへの応答個号（ＲＥＳＰ）を計算するために、各々、その移動局とネットワークのみに知られており決して空中に通信されていない、秘密の永久認証キーを用いる。移動局で発生されたＲＥＳＰは、ネットワークに通信される。

（４）ネットワークは、移動局から受信したＲＥＳＰを、内部で発生されたバージョンと比較し、そして前記比較が成功した場合のみ、登録、通話の開始または通話の受信のためのアクセスを移動局に付与する。

ＩＳ－５４では、ＭＩＮは、３４ビットの二進ワードであり、移動局の１０桁のディレクトリ電話番号、即ち、地域コードと電話番号から得られる。ＩＳ－５４の、２．３．１章、ｐｐ７８－７９を見られたい。移動局は、ランダム挑戦メモリに、オーバーヘッドメッセージ列に定

期的に添付されるランダム挑戦グローバルアクションメッセージにて受信された最後のＲＡＮＤを表わす、１６ビット値を記憶する。移動局は、これらのメッセージを用いて、ランダム挑戦メモリを更新する。ＲＡＮＤの現在値は、認証アルゴリズムＡＵＴＨ１への入力として用いられる。［ＩＳ－５４、２．３．１２章、ｐｐ８３－８４を見られたい。このように、ＩＳ－５４では、移動局がＭＩＮを送信する前に、ＲＡＮＤが移動局に送信され、１つのＲＡＮＤのみが、いかなる特定の時でも、ネットワークにおいて不正移動局を含む全ての移動局のために用いられ、これによってシステム内の機密性のレベルを低下させている。更に、ＲＡＮＤが前もって移動局に知られているので、ＲＥＳＰが事前に計算され、ＭＩＮと共にネットワークに送信される。しかしながら、ネットワークは、移動局が以前にネットワークに登録されていなければ、ＭＩＮを受信せずにＲＥＳＰを事前に計算してある可能性はない。［ＩＳ－５４システムのＡＵＴＨ１において用いられている認証キーは、各加入者のためにシステム操作者によって管理されている秘密番号である。個人的識別番号（ＰＩＮ）から成る。［ＩＳ－５４ＡＵＴＨ］は、いかなるセルラシステムに対しても移動局を唯一に識別する、工場で設定された電子連番（ＥＳＮ）も用いている。［ＩＳ－５４　ＡＵＴＨ１によって計算されるＲＥＳＰは、（ｉ）ＰＩＮ、（ｉｉ）ＥＳＮ、及び（ｉｉｉ）ダイアルされた桁（移動が発した通話に対して）またはＭＩＮ（移動が通話した通話）に、依存する。［ＩＳ－５４による移動局によって送信されたＲＥＳＰは、ＡＵＴＨ！の出力（ＡＵＴＨＲ）（１８ビット）と、ＲＡＮＤに依存するランダム課題（ＲＡＮＤＣ）（８ビット）との、合計２６ビットから成る。ＡＵＴＨＲとＲＡＮＤＣとの間で、暗号法の区別はせず、そしてこれらの値のきわは、ＲＡＮＤ、ＰＩＮ、ＥＳＮ、そして恐らく通話された番号の値に依存してもよい。したがって、ＡＵＴＨＲ及びＲＡＮＤＣは、単に２６ビットのＲＥＳＰを構成し、その独某は用いられるアルゴリズムＡＵＴＨ１によって決定されるものと、見做すこともできる。

［ＩＳ－５４によれば、移動が起こした通話設定の場合ＲＥＳＰに影響を与える、ダイアルされた桁の使用は、ある変更しないまたは正当すべき結果をもたらすが、それが以下に論められている。

（１）ダイアルされた桁が前もってネットワークに知られることはあり得ないので、ネットワークは、いかなる特定のＭＩＮのための所与のＲＡＮＤに対しても、予測されるＲＥＳＰを事前に計算することはできない。したがって、ダイアルされた桁が、移動局からネットワークに送信されるまで、認証アルゴリズムＡＵＴＨ１を実行することができないので、通話設定を遅らせる可能性がある。一方、ダイアルされた桁が含まれていないと、ＲＡＮＤが変わらないままでいる限り、同一移動局が同一ＲＥＳＰを生成する。このような場合、ＲＥＳＰを得受しかつ用いて、不正通話を行ない、ＡＵＴＨ１を有する基本的な理由をごとごとく破ってしまう可能性がある。

（２）ダイアルされた桁をＡＵＴＨ１への入力として用いると、ＲＡＮＤ及びＲＥＳＰ対の発生、そしてそれらを前もって訪問先ネットワークに送ることから、ホームネットワークを、排除することになる。

（３）このような用法は、一般的にＲＡＮＤ及びＲＥＳＰ対の前もっての事前計算を排除し、それが通話設定において時間を節約するには望ましいこともある。

（４）このような用法は、ネットワーク間、機密性に関連する通信、及びまたは認証機能の位置付けについていくらかの前提を示唆するものである。特に、これが示唆するのは、ホームネットワークが秘密キー（及びＥＳＮ）を訪問先ネットワークに送信し訪問先ネットワークが認証を実行できるようにすること、或いは、その代わりに、ダイアルされた桁が各通話毎に、訪問先ネットワークからホームネットワークに送られて、ホームネットワークが認証を実行できるようにすることの、いずれかである。ホームネットワークは、通常通話された加入者番号を前もって知る必要はないであろう。（５）［ＩＳ－５４によれば、ダイアルされた桁は暗号化されない形式で送信されなければならないので、不正移動局が同一番号に通話を行なうことも、そして「フラッシュ（ｆｌａｓｈ）」即ち協調手順を経て、彼が選択した別の番号に接続することもできる。

（６）少なくとも１つの既存ネットワークにおいて、ある番用を防止するために呼び出し先加入者非元帳、即ち、ダイアルされた桁の記載を、導入することと、ＡＵＴＨ１の定義がこのように要求される記載の便宜を図ることが必要と思われる。

本発明のシステムは、ダイアルされた桁がＲＥＳＰに影響を与えないアルゴリズムＡＵＴＨ！を定義することによって、上に述べた問題の全てに対処するものである。ＡＵＴＨ１からのダイアルされた桁の実行によって起こされるいかなる問点も、例えば、ＲＡＮＤが不変のままである際の同一ＲＥＳＰの発生も、トラフィックチャンネル上で作ることができる、第２の選択的な判断（ｂｉａｔｅｒａｌ）認証ステップを定義することによって、補償される。トラフィックデータの暗号化過程によって、更なる防護が設けられる。本発明は、ＩＳ－５４の使用を実質的に変えることなく用いることができることに、注意されたい。

ホームネットワークまたは訪問先ネットワークのどちらの場所かに係わらないことは、認証アルゴリズムを実行するにはより好都合であると考慮されるものであり、認証または暗号化が行なわれる場合、ネットワーク間での機密性に関連する加入者情報の交換は避けることができない。訪問先ネットワークがＲＡＮＤＣを定期的に決定しそして同報通信（ｂｒｏａｄｃａｓｔ）するＩＳ－

５４認証手順では、認証アルゴリズムがホームネットワーク内で実行されると、訪問先ネットワークは、ＲＥＳＰと一時的機密暗号化キー（Ｓ－キーまたは通話変数）を受信するために、少なくともＭＩＮとＲＡＮＤとをホームネットワークに送信しなくてはならない。一方、認証アルゴリズムを訪問先ネットワークにおいて実行する場合、そのネットワークは少なくともＭＩＮをホームネットワークに送信しなければならず、そしてホームネットワークは、次に、認証キー、ＥＳＮ（ＥＳＮがＡＵＴＨ１で用いられているなら）、及び永久暗号化キーを、訪問先ネットワークに送信しなければならない。機密性という観点からは、ホームネットワークが、単に訪問先ネットワークによる要求で、加入者の永久キーを放出するのは望ましくない。このようなキーは、短期間の通話変数（ｃａｌｌ　ｖａｒｉａｂｌｅ）ではなく、加入者の長期間の機密を保証するものでなければならない。したがって、訪問例（ｖｉｓｉｔｉｎｇ）移動ネットワークのＭＩＮ、訪問先ネットワークによるＲＡＮＤ同報通信、及び移動局からの訪問先ネットワークによって受信されたＲＥＳＰを、訪問先ネットワークから受信した時に、ホームネットワークが短期間の（一時的）暗号化キー（Ｓ－キーまたは通話変数）を発生し、そしてＲＥＳＰが有効と思われるならそのＳ－キーを訪問先ネットワークに放出するのが、より望ましいことである。

ホームネットワークにおける認証アルゴリズムの実行は、各移動ネットワークに対して唯一であり、ここではＡ－キーと呼ぶ長期間（永久）秘密キーを、認証アルゴリズムが用いることができるようにする。Ａ－キーは、ホームネットワーク外には決して放出されず、暗号化には直接使用されないが、代わりに、ここではＳ－キーと呼ぶ短期間の暗号化キーを発生するために用いられる。Ｓ－キーは、訪問先ネットワークによって決められる限られた時間期間のみ、用いられるものである。訪問先ネットワークが、以前に登録済みの訪問例移動局に対してＳ－キーを既に獲得している場合、第１の認証ステップの実行は選択的であり、通話設定は、暗号化されたトラフィックチャンネルに直接移行してもよい。したがって、訪問例移動局が通話を行なう等に、ネットワーク間交換が生じる必要はない。一方、訪問先ネットワークが、ＡＵＴＨ１による認証ステップを要求することを決めた場合、移動局及びホームネットワークは、訪問先ネットワークのＲＡＮＤを用いて新たなＳ－キーを発生するが、ＡＵＴＨ１へのその他の入力は無変化である。

認証アルゴリズムの暗号分析的特性

次に第７図を参照すると、ＩＳ－５４による認証アルゴリズムの図式表現をここに見ることができる。移動局によって通話が開始されると、移動局はそのＰＩＮまたは認証キー、そのＥＳＮ、ＲＡＮＤ及びダイアルされた桁を用いて、認証アルゴリズムＡＵＴＨ１にしたがって、ＲＡＮＤへの応答を計算する。移動局は、次に、ＡＵＴＨＩの出力（ＡＵＴＨＲ）を、ランダム論題（ＲＡＮＤＣ）、ダイアルされた桁、移動局の個々の通話履歴パラメータ（ＣＯＵＮＴ）及びＭＩＮと共に、ネットワークに送信する。ダイアルされた桁に、移動が発した通話において認証応答（ＡＵＴＨＲ及びＲＡＮＤＣ）に影響を与えさせた結果は、先に論じており、望ましくなきものと思われる。一方、通話された加入者の身元を隠蔽する可能性の保証を図ることは、望ましいものと考慮される。移動にて終了した通話の場合、ＰＩＮ／キーは十分に移動に特定的（ｍｏｂｉｌｅ－ｓｐｅｃｉｆｉｃ）であるので、ＭＩＮを用いることによって認証応答に影響を及ぼすものは得と得られない。

次に第３図を参照すると、本発明による暗号化アルゴリズムの図式表現が見られる。移動が発した通話の場合にダイアルされた桁も、移動にて終了した通話の場合のＭＩＮも、ＡＵＴＨＩへの入力として用いられていない。更に、本発明によるＡＵＴＨＩの出力は、認証応答だけでなく、移動によって起こされた通話の場合のダイアルされた桁を確認するのに用いることができる、被通話加入者確認（ｃａｌｌｅｄ　ｓｕｂｓｃｒｉｂｅｒ　ｍａｓｋ）も、含んでいる。ＡＵＴＨＩの特定の実施例を、以下に記載し説明する。

移動局は、貴方されたり、盗まれたり、合法的に獲得されたりすることがあり、そのＥＳＮ、秘密キー、ＰＩＮコード等を含むそのメモリ内容全体がコピーされ、そして多数のクローンを製造するために用いられることもあり得る。クローン化手順は非常に洗練されているかもしれず、そして物理的に記憶されたＥＳＮ情報を電子的に記憶された情報と置換するソフトウエアの改造を含んでおり、多数の記憶された移動局の身元が、１つの不正移動局内で巡回的に回転され、そしていくつかの本当の移動局を模倣するために用いられる可能性もある。

通話の付番は、ネットワークにクローンが存在するか識別できるようにする手段として、採案されている。通話の付番において、モジュロ－６４カウントが移動局内で続けられ、各通話の後またはネットワークによって命合された時に、増分される。同様のカウントが、ネットワーク内でも続けられている。移動局はその通話番号をネットワークに、通話の確認（ｓｔｅｐ－ｕｐ）時に送信し、ネットワークは受信した通話番号を、内部で発生したものと比較する。この比較は、しかしながら、幾つかの理由の１つのために、できないことがある。

（１）停電のような異常な終了のため最後の通話の後に、移動局がその通話カウントを更新しなかった。

（２）移動局はその通話カウントを更新したかもしれないが、ネットワークが、異常な終了のため、移動局がそうしたことの識認を受信しなかった。

（３）クローン移動局が１回異常の通話を行ない、ネットワークカウンタを進めた。

（４）移動局自体がクローンであり、一方で「本当の」

移動局がカウンタを進めた。

残念なことに、通話カウンタはいずれの方向にも余り簡単に修正されてしまうので、前述の状態のどれが発生したのかをネットワークは判断できず、したがってネットワークは移動局へのサービスを否定することを強制され得ない。このような悪意の結末を回避するために、移動の加入者は、例えば、移動局のメモリには記憶されていない、短い秘密番号をキー入力することによって、手動で彼自身または彼女自身をネットワークに対して識別する付加的な機会を与えられている。本発明のシステムは、動的な「ローリングキー」を基にした別の対クローン化防護を提供するが、これはホームネットワーク及び移動局の各々に記憶されており、そして認証応答及び一時的暗号化キーを計算するために、永久秘密キーと共に用いられるものである。このようなローリングキーが認証のみのために以前に用いられたことがあるが、それらは認証及び暗号化パラメータの両方を生成するために用いられたのではなかった。

ローリングキーの概念の背景にある原理は、クローンに対する防御手段として、そして移動局メモリの理解で高価な物理的防御を要求する代わりに、各ネットワーク及び移動局内のある履歴情報を照合することを必要としている、ということである。具体的には、クローン移動局がシステムへのアクセスを得るためには、そのクローンは、本当の移動局のその時の現行キー状態をコピーした時点に続いて、認証機能の全履歴を得受することが必要となる。本発明によれば、認証はホームネットワーク内で、ここではＢ－キーとよばれるローリングキーの組み合わせを用いて行なわれ、これは履歴情報及び永久秘密加入者キー（Ａ－キー）を含んでおり、そして暗号化アルゴリズムに直接もちいられることは決してなく、１つ局得の動作用擬密キー（ｏｐｅｒａｔｉｎｇ ｓｅｃｕｒｉｔｙ ｋｅｙ）を発生するためのみに用いられるものである。本システムの認証アルゴリズムは、移動局とホームネットワークとが更新について同意した時はいつでも、ローリングキーの現在値になり、ローリングキーの新しい値も計算する。このような更新は、以下に更に述べる両方向認証手順の実行のために、訪問先ネットワークまたはホームネットワークからの要求によって、開始され得るものである。

ローリングキーの更新は、訪問先ネットワークが、ホームネットワーク及び移動局において通話カウンタを更新することを決めたとき、会話中いつでも、実行することができる。その通話カウンタを更新する前に、ホームネットワークは、移動局の両方向認証を要求することができる。そして、移動局からの正常な応答の結果、通話カウンタの更新、ローリングキーの更新、及び以後の通話に用いるために訪問先ネットワークに送られる新しい会話擬密キー（Ｓ－キー）の発生が行なわれる。同様に、移動局も、両方向認証手順が、訪問先ネットワークがホームネットワークと本局に接触していることを確認した場合のみ、その通話カウンタを更新することができる。確認の際、移動局は、その通話カウンタ及びローリングキー（Ｂ－キー）も更新し、同じ訪問先ネットワークによって供給される以後の通話に用いるための新しい会話機密キー（Ｓ－キー）を発生する。通話カウンタとローリングキーとが同時に更新されるので、移動局及びホームネットワークの通話カウンタのチェックが、移動局及びホームネットワークが同一ローリングキー状態にあるかの指示としても、役立つことになる。

両方向認証

両方向認証即ち移動局とネットワーク両方の認証が、一方向認証と区別されるのは、前者では両方向に送られる認証情報がキーに依存するのに対して、後者では移動局からネットワークへの方向に送られる情報のみがキーに依存する点においてである。本発明によれば、ＲＡＮＤ信号が認証アルゴリズムＡＵＴＨ２への入力として用いられ、これは及いＲＥＳＰ信号を発生し、その一部がネットワークから移動局に送られてネットワークを有効化すると共に、他の部分が移動局によってネットワークに送られて移動局を有効化する。例えば、アルゴリズムＡＵＴＨ２は、ＲＡＮＤからＲＥＳＰを計算し、次に違んでＲＥＳＰをアルゴリズムＡＵＴＨ２への新しいＲＡＮＤ入力として用いることができ、これが次にＲＥＳＰＢＩＳ信号を計算する。ネットワークは、ＲＡＮＤ及びＲＥＳＰＢＩＳを移動局に送信し、これがＲＡＮＤを用いてＲＥＳＰとＲＥＳＰＢＩＳとを、ＡＵＴＨ２にしたがって計算する。移動局は、内部で発生したＲＥＳＰＢＩＳがネットワークから受信したＲＥＳＰＢＩＳに一致する神のみ、内部で発生したＲＥＳＰをネットワークに送る。これは、不正基地局が移動局からＲＡＮＤ、ＲＥＳＰ対を抽出するのを防止するものであり、移動局とネットワークの各元の確認によって、機密状態の更新が、比較的安全に、好都合な後の点に移行することができる。

暗号化キー（通話変数またはＳ－キー）の発生

通信の暗号化が、訪問先ネットワークにおいて望まれる時、暗号化キーを、ホームネットワークから訪問先ネットワークに通信しなければならない。先に述べたように、永久秘密加入者Ａ－キーが特に保護されていないリンク上でネットワーク間を巡回することは、非常に望ましくない。代わりに、そして本発明によれば、ホームネットワークは、所与の加入者のＡ－キーを決して放出せず、一時的トーク変数（ｔａｌｋ－ｖａｒｉａｂｌｅ）擬密キー（Ｓ－キー）を発生するためのみにＡ－キーを用いており、次に特定の通話または通話群を暗号化するための擬似ランダムキーストリームを発生するために、それが用いられる。本発明の擬似ランダムキーストリーム発生技術についての元の議論において言及した「秘密キー」は、暗号化に直接用いられるＳ－キーを選わしたのであって、Ｓ－キーが得られる永久秘密Ａ－キーのこ

とではない。有効なＭＩＮ、ＲＡＮＤ、及びＲＥＳＰを受信した時に、このＳ－キーを計算してホームネットワークから訪問先ネットワークに送る。

Ｓ－キーは、認証挑戦－応答信号（ＲＥＳＰ）と同時にそして同じ過程によって計算されるので、成功した認証は、ネットワークと移動局が同一暗号化キー（Ｓ－キー）を有し、そして結果的に認証が完了するとすぐにユーザデータの暗号化が開始できることを保証する。したがって、本発明のシステムにおける認証と暗号化との連係は、移動局及び基地局によって識別されなければならない異なる機密－機構の組み合わせの数を、四（４）から二（２）に減少させることがわかるであろう。

入力及び出力ビットカウント

トーク変数（Ｓ－キー）は、上述のＲＥＳＰ及びＲＥＳＰＢＩＳパラメータを生成したのと同じ認証アルゴリズムの副産物として発生される。このようなアルゴリズムからの他の所望の出力は、（ｉ）通話された加入者番号を確認するのに十分なビット、及び（ｉｉ）ネットワークが両方向認証によって有効化され、及び／または通話カウンタ更新命令が発行された場合に、現状態を置換するローリングキー（Ｂ－キー）の次の状態を、含む。

例として、そして本発明の教示に対する制限はしないものとして、次の表はアルゴリズムの出力に対する、ビット及びバイトカウントを例示したものである。

出力	ビット数	バイト数
ＲＥＳＰ	３２	４
ＲＥＳＰＢＩＳ	３２	４
通話された番号確認	６４	８
Ｓ－キー	６４	８
次のＢ－キー	６４	８
合計ビット	２５６ 合計バイト	３２

次の表は、アルゴリズムの入力に対するビット及びバイトカウントを例示したものである。

入力	ビット数	バイト数
Ａ－キー	１２８	１６
Ｂ－キー	６４	８
ＲＡＮＤ	３２	４
ＥＳＮ	３２	４
ダイアルされた桁	０	０
合計ビット	２５６ 合計バイト	３２

上に示した値は、３２ビット入力及び３２ビット出力を有するアルゴリズムを与えるために、故意にためたものである。これより短い変数を用いる場合、変数を用いて低減すればよい。先の入力及び出力バイトカウントを有し、移動局に一般的に見出される形式の簡素な８ビットマイクロプロセッサにおける、バイト幅動作による高速実行に相応しいアルゴリズムを、「認証アルゴリズムの定義」と題された別項の末で、以下に記載する。

本認証システムの一般的特性

本発明は、ネットワーク操作者の自由に用いることができる、認証の２つのステップを提供する。第１のステップは、先の説明でＡＵＴＨ１と呼ばれていたものである。認証アルゴリズムの定義と題された章で記載されるアルゴリズムは、ＡＵＴＨ１のために用いられる。このようなアルゴリズムでは、ダイアルされた桁は、出力に影響を与えない。制御チャンネル上の１６ビットＲＡＮＤ同報通信が用いられ、３２ビットの入力を与えるために２度含まれる。このアルゴリズムの出力パラメータは、移動局によって通話チャンネル上のネットワークに送られるＲＥＳＰとＭＩＮと、ＴＤＭＡトラフィックチャンネルに切り換えた時直ちにユーザデータを暗号化するのに用いることができる通話変数（Ｓ－キー）とを含む。移動が発した通話の場合、通話された加入者番号を確認するために、付加的な出力パラメータが与えられる。このパラメータは、ホームネットワークから訪問先ネットワークに送られ、通話された番号の確認を解くことができるようになっている。

先の説明では、ＡＵＴＨ２と呼ばれていた第２の認証ステップは、一旦通信がトラフィックチャンネル上に確立されると、ネットワークの自由に進行することができる両方向認証である。両方向認証ステップの目的は、移動局及びホームネットワークの両方でのローリングキー（Ｂ－キー）の更新を開始し、同時にそれらを互いに有効化することであり、こうしてある形式の不正基地局のシステムの機密性への攻撃を防止している。ＡＵＴＨ２のアルゴリズムは、以下の認証アルゴリズムの定義と題された章に記載されたＡＵＴＨ１のアルゴリズムと、ＲＡＮＤ値がホームネットワークによって決定され、ＲＥＳＰＢＩＴと共に訪問先ネットワークに送られ、そしてそこから移動局に送られることを除いて、同一である。移動局がＲＥＳＰＢＩＳを有効化すると、移動局はＲＥＳＰを訪問先ネットワークに送り、これがＲＥＳＰをホームネットワークに送る。ホームネットワークがＲＥＳＰを有効化した場合、ホームネットワークは、訪問先ネットワークに、次の通知のために用いることができるＳ－キーを送る。　次に第９図を参照すると、本発明の認証アルゴリズム及び暗号化技術を用いた移動セルラシステムの図式表現がそこに示されている。従って、１台の移動局、１台の訪問先ネットワーク及び１台のホームネットワークのみが、第９図に描かれているが、実際には多数の移動局、訪問先ネットワーク及びホームネットワークが通常見出されることが、理解されよう。第９図に見られる以下の略号は、次の用語からきたものである。

Ａ１及びＡ２	夫々ＡＵＴＨ１及びＡＵＴＨ２
Ａ３	本発明に依る暗号化技術
ＩＶＣＤ	初期音声チャンネル指定
ＭＳ	移動局
ＶＬＲ	訪問先ネットワーク
ＨＬＲ	ホームネットワーク

第9図において、訪問側ネットワークは、新しいＲＡＮＤＩ値を、そのサービス領域内の全移動局に、定期的に同報通信する。移動局の各々は、応答ＲＥＳＰＩを計算し、これがＭＩＮ及び通話識別パラメータＣＯＵＮＴと共に訪問先ネットワークに送られる（いくつかの用途では、ＲＥＳＰＩ、ＭＩＮ及びＣＯＵＮＴは到価に送られることもあることに注意されたい）。訪問先ネットワークは、移動局のホームネットワークからの特定の移動局に対する暗号化キー（Ｓ－キー）を要求する。ホームネットワークは、ＲＡＮＤＩ、ＥＳＮ、Ａ－キー及びＢ－キーを、認証アルゴリズムＡＩに適用することによって、それが得たパラメータと受信した応答を比較し、当該移動局が本物かを判断し、それにしたがってホームネットワークは一時的暗号化キー（Ｓ－キー）を訪問先ネットワークに放出する。訪問先ネットワークが暗号化キーを受信しない場合、訪問先ネットワークは移動局へのサービスを否定することができる。

訪問先ネットワークがアクセスを付与し、ＴＤＭＡチャンネル（または幾つかの周波では制御チャンネル）を移動局に割り当てると、そのチャンネルを定義するパラメータ、即ち、周波数、タイムスロット及びＤＶＣＣが、訪問先ネットワークから移動局に送られ、割り当てられたトラフィック（または制御）チャンネルに同調させる。その後、訪問先ネットワークと移動局とは、Ｓ－キーを用いて暗号化モードで通信することができる。先に利用して暗号化され続ける。ハンドオーバーまたは通話の終了時に、この新しいＳ－キーが使用され始める。

認証アルゴリズムの記載

記述の概要

本発明の認証アルゴリズムは、通話例チャンネルでの認証（ＡＵＴＨ１）と、トラフィックチャンネルでの両方向認証（ＡＵＴＨ２）との両方に、用いることができる。アルゴリズムの例示的コーディングが、幾つかの一般的なマイクロプロセッサの実施に対して、与えられる。以下に続く記述では、アルゴリズムの入力及び出力変数に対して、あるバイトカウントが選択されている。しかしながら、このようなバイトカウントは、単に例示であり、本認証アルゴリズムの適用性に対する限定を意図したものでもなければ、そう解釈すべきでもないことは、明白に理解されよう。

アルゴリズムの入力及び出力変数

本発明のシステムのアルゴリズムは、合計３２バイトの入力信号を用い、３２バイトの出力パラメータを発生する。これは、１６バイトの入力変数を用い、１６バイトの出力変数を発生するアルゴリズムを２回通用することによって、達成される。この入力変数は、

ＲＡＮＤ：　４バイトまでに対して設けられる］
　　ＮＯＮ－ＳＥＣＲＥＴ
ＥＳＮ：　４バイトまでに対して設けられる］
　　ＶＡＲＩＡＢＬＥＳ

し、参考として組み込まれた「セルラ通信システム用連続時号同期」と題する、関連する係属中の特許出願に記載されているように、訪問先ネットワークは、そのフレームカウンタを、暗号解除されたＳＡＣＣＨを通じて送り、そして固定鍵の暗号解除されたＡＣＣＨメッセージも送る。ＦＡＣＣＨのシグナリング（ｓｉｇｎａｌｌｉｎｇ）またはトラフィックの要なる交換が、暗号化モードにおいて生じることがある。

両方向認証及びローリングキーの更新

一旦移動局と基地局とが、トラフィックチャンネル上で通信を確立すると、訪問先ネットワークは、いつでも、両方向認証の実行、並びにローリングキーと通話カウンタの更新を、移動局にＲＡＮＤ２及びＲＥＳＰ３を送ることによって、要求する。移動局は、ＲＡＮＤ２、ＥＳＮ、Ａ－キー及びＢ－キーを用いて、予測されるＲＥＳＰ３及びＲＥＳＰ２を発生する。内部で発生したＲＥＳＰ３が、受信したＲＥＳＰ３と同一であれば、移動局は、ＲＥＳＰ２を訪問先ネットワークに送る。訪問先ネットワークは、ＲＥＳＰ２をホームネットワークに送り、そしてホームネットワークの内部で発生したＲＥＳＰ２が受信したＲＥＳＰ２と同一であれば、新しく計算した通話変数Ｓ－キーがホームネットワークから訪問先ネットワークに送られる。訪問先ネットワークは、訪問制移動局に関連する将来の通話に用いるために、このＳ－キーを記憶する。現在の通話は、古いＳ－キーを用い

Ｋａ：１６バイトの永久キー（Ａ－キー）］
　　ＳＥＣＲＥＴ
Ｋｂ：８バイトのローリングキー（Ｂ－キー）　］
　　ＶＡＲＩＡＢＬＥＳ

３２の出力バイトは、以下のパラメータとしてシステム内で用いるために、指定される。

０－３　　：認証応答（ＲＥＳＰ）
４－７　　：ＲＥＳＰＢＩＳ
　　（両方向認証に必要とされる）
８－１５　：通話または加入者番号の隠蔽
　　（もし使われるなら）
１６－２３：キー更新が生じた場合、次のＫｂ
２４－３１：この通話を暗号化するためのトーク変数（Ｓ－キー）

３２バイトのアルゴリズムへの入力は、１６バイトのグループに分割され、これらがアルゴリズムの幾何の用途において用いられ、第１の１５バイトの出力（バイト０－１５）を生成する。次に、３２バイトの入力は、同の方法で分割されて、アルゴリズムの２番目の用途に用いられ第２の１６バイトの出力（バイト１６－３１）を生成する。

アルゴリズムの全体的構造

本アルゴリズム（コード）は、セルラ無線電話にて用いられる形式の簡素なマイクロプロセッサ上での、非常に効率的かつ高速な実行のために構成されたものである。

小さな内部コードループを繰り返し用いることが、コードを１６０バイト領域内に制限するのに役立っている。外部ループは、混合過程を５項目繰り返し実行することから成る。混合過程は、第１０図に示されている。

次に第１０図を参照すると、本発明の最近アルゴリズムに用いられる混合過程の機能ブロック図がそこに示されている。混合過程３００は、１６個のキーバイトの第１の入力と、１６個の入力バイトの第２の入力とを、備えている。最初の繰り返しに対する１６入力バイトは、次の順序の４バイトのＲＡＮＤ、４バイトのＥＳＮ、及び８個のローリングキーバイトＫｂ（０－７）から成る。

ＲＡＮＤ　４バイト（１６ビットのＲＡＮＤが２回繰り返されている）

ＥＳＮ　４バイト

Ｋｂ（１）

Ｋｂ（２）

Ｋｂ（３）

Ｋｂ（４）

Ｋｂ（５）

Ｋｂ（６）

Ｋｂ（７）

Ｋｂ（０）

混合過程の各繰り返しに対する入力として設けられた１６個のキーバイトは、８個のローリングキーバイトＫｂ（０－７）と１６個の永久キーバイトＫａ（０－１５）からの巡回式選択である。アルゴリズムの最初の用途では、１６個のキーバイトの使用順序は、以下の通りである。

繰り返し番号	用いられるキーバイト
1	Ka(0)--->Ka(15)
2	Kb(0)--->Kb(7);Kb(0)--->Kb(7)
3	Ka(8)--->Ka(15);Kb(0)--->Kb(7)
4	Kb(4)--->Kb(7);Ka(0)--->Ka(11)
5	Ka(4)--->Ka(11);Kb(0)--->Kb(3)

上述のキー再生、即ちキー変数を一時的メモリ領域にＫｂ、Ｋａ、再びＫｂの順にコピーし、そしてそれらを連続的に各繰り返しに対して適切な場所から開始してこのメモリから選択することにより、得ることができる。

アルゴリズムの混合過程

混合過程３００は、１６個のキーバイトと１６個の入力バイトを対にして、例えばバイト桁加算命令を用いて、組み合わせる。また、混合過程３００は、ランダム１：１置換ボックスまたは、以後Ｓ－ボックスと呼ぶことにする参照テーブル、を用いて、１バイト値を別の１バイト値に変換する。Ｓ－ボックスは、本システムのキーストローク発生器によって用いられ、パラメータＲの原として第５－６図に関して先に論じたのと同じ参照テーブルであることが、好ましい。Ｓ－ボックスは、マイクロプロセッサのプログラムメモリに含まれている２５６バイトのリードオンリメモリ（ＲＯＭ）によって、実施することができる。１：１Ｓ－ボックスは、各８ビット入力値が唯一の８ビット出力バイトを生成する、または言い換えれば、各可能性のある８ビット値がテーブル内に１度しか現われないことを意味する。これは、一様でない値の分布を回避するために望ましいものである。あるマイクロプロセッサでは、Ｓ－ボックスのアドレッシングが真で位アドレスバイトの操作のみを必要とするように、Ｓ－ボックスが２５６バイトページの境界に来るように構成すると、プログラミングタスクが幾分低減される。

次に第１１図を参照すると、混合過程の機能ブロックまたは混合セルの機能ブロック図がここに示されている。混合過程は、通常第１１図に示した形式の複数の混合セルまたは内部ループから構成することができる。第１０図に示す特定の混合過程は、１６個のこのような混合セルの並直な積み重ねとして、視覚化することができる。これらのセルの各々は、加算器３１０によって共に加算される、１つのキーバイトと１つの入力バイトとが備えられている。加算器３１０の出力を用いてＳ－ボックス３２０の内容をアドレスし、これが加算器３１０の出力によって定義されたアドレスに記憶されている出力バイトを放出する。混合セルまたは内部ループのソフトウエアの実施を、以下「インテル」及び「モトローラ」のアーキテクチャのマイクロプロセッサに対して、記載する。

アルゴリズムの第２の用途

アルゴリズムの第２の用途は、会話キー（Ｓ－キー）、そして、実行されるのであれば、ローリングキー（Ｂ－キーまたはＫｂ（０－７）の更新のために用いることができる１６個の出力バイトの第２のグループを発生する。アルゴリズムの第２の用途は、キーバイト及び入力バイトが用いられる順序を除いて、第１の用途と正確に同一である。アルゴリズムの第２の用途では、１６個のキーバイトの使用順序は、次の通りである。

繰り返し番号	用いられるキーバイト
1	Kb(0)--->Kb(7);Ka(0)--->Ka(7)
2	Ka(8)--->Ka(15);Kb(0)--->Kb(7)
3	Kb(4)--->Kb(7);Ka(0)--->Ka(11)
4	Ka(4)--->Ka(11);Kb(0)--->Kb(3)
5	Ka(0)--->Ka(15)

加えて、１６ビット入力アレイが、Ｋｂバイトの代わりにＫａバイトを用いて以下のように、初期化される。

ＲＡＮＤ（０）

ＲＡＮＤ（１）

ＲＡＮＤ（０）

ＲＡＮＤ（１）

ＥＳＮ（０）

ＥＳＮ（１）

ＥＳＮ（２）

ＥＳＮ（３）

Ｋａ（７）

Ｋａ（８）

Ｋａ（９）
Ｋａ（１０）
Ｋａ（１１）
Ｋａ（１２）
Ｋａ（１３）
Ｋａ（１４）

アルゴリズムの第２の用途の５回の繰り返し全てを実行した後、１６バイト入力アレイ内の２番目８バイトが、一時的暗号化変数（Ｓ－キー）として用いられ、そして、ローリングキーの更新が実行されると、最初の８バイトが次のローリングキー変数となる。ローリングキーの更新の際、最初の８個の出力バイトが、Ｋｂ（１）、Ｋｂ（２）、Ｋｂ（３）、Ｋｂ（４）、Ｋｂ（５）、Ｋｂ（６）、Ｋｂ（７）、Ｋｂ（０）の順で、古いローリングバイトを上書きする。

Ｓ－ボックスの内容

以下に記載するＳ－ボックスの内容は、例示するのみであり、本発明の認証及び暗号化システムの更なる説明において与えられるものである。先に述べたように、認証アルゴリズムにおけるＳ－ボックスは、本発明の暗号化技術に用いられるＲ参照テーブルと同一でもよい。Ｓ－ボックスの内容を、以下に１６進表記で表わす。最初のバイト（値＝５０）は、場所０、即ちＲＯＭの開始アドレスにある。第１ラインのデータ（１６の値）は、場所０から１５に記憶され、後続のラインのデータは、夫ＲＯＭのそれに続く１６箇所に記憶される。

アドレス	データ															
(00)	50	02	F1	C8	3E	21	08	1C	A5	F6	9A	81	10	4A	3C	34
(10)	C8	F9	C0	77	20	83	F6	88	E2	BC	69	71	EC	48	48	65
(20)	5C	04	66	8C	78	13	CA	99	AD	5E	61	AD	BC	61	EA	2C
(30)	8F	94	87	06	40	AA	74	18	36	B7	4C	68	35	10	28	EF
(40)	E4	45	B6	E0	D7	AE	5D	23	F4	CE	E9	70	E8	54	54	F7
(50)	5A	22	8E	A6	83	9F	26	67	32	E1	C2	E8	93	E5	BF	3F
(60)	A8	38	41	47	25	D6	29	C3	00	C8	07	8F	86	1A	66	69
(70)	59	C0	80	BA	62	0A	1E	87	18	58	CF	30	2D	37	61	7C
(80)	42	62	80	A2	83	84	95	6E	73	5A	5A	58	B0	9D	A5	98
(90)	4D	E3	48	0C	C1	3E	E6	7F	62	DF	33	A1	2F	8E	3A	7E
(A0)	ED	C5	F2	F0	D3	66	78	90	08	76	E7	BE	2E	C4	7A	A6
(B0)	4F	AF	A7	86	63	91	34	17	F7	39	96	D6	56	CC	D9	30
(C0)	31	F3	82	68	F9	0F	07	39	A6	D2	19	DD	43	83	00	FE
(D0)	92	08	18	6F	12	01	6C	A4	1F	A3	40	B4	06	4E	DE	FA
(E0)	11	84	C8	46	60	14	28	96	EE	50	FC	DC	70	88	72	01
(F0)	55	2A	05	D3	27	44	AC	8A	83	78	09	F8	79	C7	D0	F0

マイクロプロセッサの一般的形式用コーディング例

８０８０／８０８５　及びＺ８０　コード

固定ＲＯＭ即ちＳ－ボックスは、１６ビットレジスタＤＥによってアドレスされたページ境界上に配置された２５６バイトのテーブルである。

```
CELMIX:   LDAX B   ;BC REGISTER IS USED TO POINT TO KEY
                    BYTES
          ADD  M   ;THE HL REGISTER POINTS TO INPUT BYTES
          MOV  E,A ; THE SUM OF A KEY BYTE AND AN INPUT BYTE
          LDAX D   ;ADDRESSES THE S-BOX
          MOV  M,A ;OUTPUT BYTE FROM S-BOX OVERWRITES INPUT
                    BYTE
          INX  H   ;NEXT INPUT BYTE ADDRESS
          INX  B   ;NEXT KEY BYTE ADDRESS
          RET
```

上記ルーチンは、次のように用いられる。

（１）Ｄレジスタを、ページ境界にあるＳ－ボックスの開始アドレスのＭＳＢにセットする。

（２）先に述べた繰り返し数にしたがって、キーバイトのアレイ内の適切な開始アドレスにＢＣを初期化する。

（３）入力バイトの１６バイトアレイへのポイントにＨＬを初期化する。

（４）ルーチンを１６回実行する。

直前のステップは、上記混合過程の１回の繰り返しを実施するものである。最初の繰り返しに先立ち、ＲＡＮＤ、ＥＳＮ及びＡ－キー及びＢ－キーバイトの先に示した選択を用いて、１６バイトの入力アレイが初期化される。

１６個の出力バイトは、元の入力バイトアレイにあり、次の繰り返しに対する入力のために使用可能となっている。先に示したキーバイトの選択を用いて５回の繰り返し全てを実行した後、１６個の出力バイトは、アルゴリズムの所望の出力を表わしている。

６８０９用コード

```
CELMIX:   LDA  ,X+   ; THE X REGISTER IS USED TO POINT TO
                        KEY BYTES
          ADDA ,Y    ;THE Y REGISTER POINTS TO INPUT
                      BYTES
          LDA  A,U   ;U=ADDRESS OF S-BOX START, A=OFFSET
                        FROM START
          STA  ,Y+   ;BYTE FROM S-BOX OVERWRITES INPUT
                      BYTE
                        RET
```

＋は、指示されたレジスタの使用後の自動増分を意味する。このルーチンは次のように用いられる。

（１）Ｕレジスタを S－ボックスの先頭にアドレスするようにセットする。

（２）先に述べたキーバイトの使用順序にしたがって、適切なキーバイトへのポインタに、Ｘレジスタを初期化する。　（３）１６バイト入力バイトアレイの先頭へのポイントにＹレジスタを初期化する。

（４）ルーチンを１６回実行する。

直前のステップは、第１０図に示した混合過程の繰り返しを１回実施するものである。最初の繰り返しに先立って、先の例におけるように、ＲＡＮＤ、ＥＳＮ及びＡ－キーまたはＢ－キーの指定された選択を用いて、１６

バイト入力アレイが初期化される。したがって、Yレジスタを入力バイトアレイの先頭に再初期化し、そして、残りの4回の繰り返しを実行する前に、各ステージに対する適切なキーバイトへのポインタにXレジスタを再初期化することのみが、必要となる。5回目の繰り返しの後、16バイトの入力アレイは、認証、そして、もし実施されたのなら、加入者の身元隠蔽に用いられるアルゴリズムの第1の周波からの16個の出力バイトを含んでいる。

上述のことから、本発明のシステムには、多数の概念が実施されていることが、認められよう。これらの概念の中で、認証キーのある部分（即ち「ローリングキー」部分）を定期的に更新して、複製物がシステムの機能を追跡しなければならないようにすることが、主たるものである。両方向認証がトラフィックチャンネルにおいて用いられ、セルカウンタの更新に連係されたローリングキーの更新を行なう。

本発明の認証アルゴリズムの実行が、後続の通話または通話グループを暗号化するために用いることができる、一時的会話キー即ち「トーク変数」機密キー（Sーキー）も発生すること、及び実際の秘密永久加入者キー（Aーキー）は、ホームネットワークによって決して放出されないことも、判るであろう。加えて、本発明のアルゴリズムは、通話された加入者の身元を隠蔽するために用いることができる別の出力を生成する。

これまでの記述は、本発明のある特定の実施例のみを示すものである。しかしながら、本発明の精神及び範囲から実質的に逸脱することなく、多くの修正及び変更を行なうことができることを、当業者は認めるであろう。したがって、ここに記述した本発明の形式は、例示に過ぎず、以下の請求の範囲に規定した本発明の範囲に対する限定として意図されたものでないことは、明瞭に理解されよう。

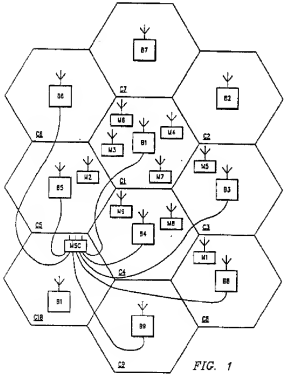


FIG. 1

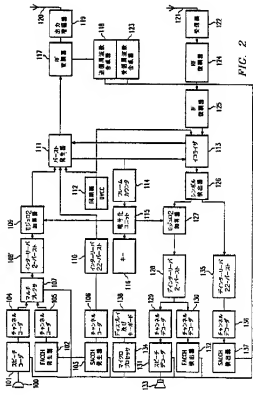


FIG. 2

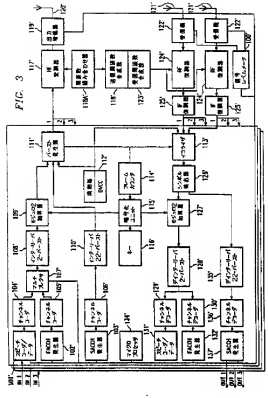


FIG. 3

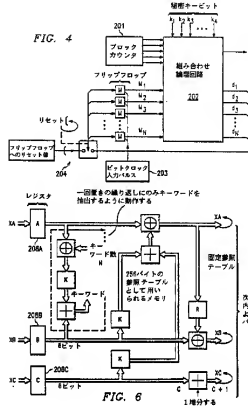


FIG. 4

FIG. 6

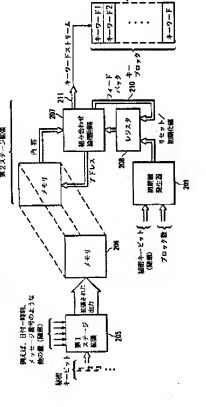


FIG. 5

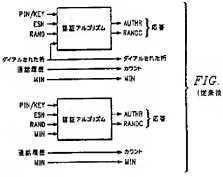


FIG. 7
(従来技術)

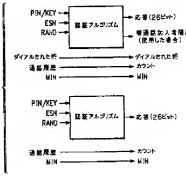


FIG. 8

FIG. 9

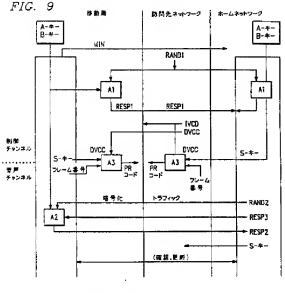


FIG. 10

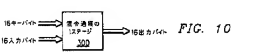
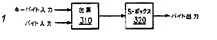


FIG. 11



平成5年8月24日

特許庁長官殿

1.事件の表示
平成3年特許願第514449号

2.発明の名称
デジタルセルラ通信用認証システム

3.補正をする者
事件との関係 特許出願人
名称 エリクソン ジーイー モービル コミュニケーションズ インコーポレイテッド

4.代理人
居所 〒100東京都千代田区大手町二丁目2番1号 新大手町ビルヂング331
電話(3211)3651(代表)
氏名 (6669) 浅村 皓

5.補正により減少する請求項の数 5

6.補正の対象
明細書
請求の範囲

7.補正の内容 別紙のとおり

8.添付書類の目録
同時に出願審査請求書を提出しております。

特許庁 5.9.22 出願係

1. 請求の範囲を別紙の通り補正する。
2. 明細書を次の通り補正する。
(1) 明細書第1頁第7行の「556,358」を「07/556,358」に補正する。
(2) 明細書第1頁第9行の「556,102」を「07/556,102」に補正する。
(3) 明細書第1頁第11行の「556,103」を「07/556,103」に補正する。
(4) 明細書第15頁第20行の「レイストレーション」を「登録」に補正する。
(5) 明細書第16頁第16行の「三(3)」を「3」に補正する。
(6) 明細書第21頁第3行の「110」を「111」に補正する。
(7) 明細書第21頁第5行の「/4-」を「π/4-」に補正する。
(8) 明細書第21頁第5行の「(/4」を「(π/4」に補正する。
(9) 明細書第21頁第11行の「/4」を「π/4」に補正する。
(10) 明細書第21頁第11行の「3/3」を「3π/4」に補正する。
(11) 明細書第21頁第25行の「/4」を「π/4」に補正する。
(12) 明細書第27頁第15～16行の「_____」を「07/556,102」に補正する。
(13) 明細書第36頁第4行の「bitwize」を「bitwise」に補正する。
(14) 明細書第36頁第14行の「ティーブル(tible)」を「テーブル」に補正する。
(15) 明細書第61頁第3行の「5項目」を「5回」に補正する。

請求の範囲

1. 通信システムにおける通信の機密性を強化するために用いられるパラメータを発生させる方法であって、移動局には固有の多数桁永久キーが割り当てられ、可変の多数桁ローリングキーが機密性を高めるために用いられており、前記永久キーと前記ローリングキーの両方は、前記移動局とその移動のネットワークに記憶されており、

該ネットワークからの認証問い合わせを表わす信号を含む複数の多数桁入力信号を、特定の移動局の多数桁永久キー及びその特定の時刻に前記特定の移動局に関連する多数桁ローリングキーと共に、ある位置で受信する段階と、

前記入力信号の桁の内の少なくともいくつかを第1の集合（ｇｒｏｕｐｉｎｇ）に構成する段階と、

前記入力信号の第1の集合と前記永久及びローリングキーの桁から、第1のアルゴリズムに従って、第1の出力値を計算する段階と、

前記第1の出力値を含む連続的に構成した桁のブロックを、該ネットワークによる認証の問い合せに対して応答するために前記移動局によって用いられる認証応答及びそれを該移動局に対して認証するために該ネットワークによって用いられる認証信号とを含む、前記システム内で用いるための選択されたパラメータに割り当てる段階と、

を含んでいる前記方法。

2. 通信システムにおける通信の機密性を強化するために用いられるパラメータを発生させる、請求項1記載の方法において、

前記第1の出力値を含む前記連続的に構成された桁のブロックが割り当てられる、前記システム内で用いるための該出力パラメータが、該移動局によって送信される情報をマスクするために用いられる信号をも含んでいる、前記方法。

3. 通信システムにおける通信の機密性を強化するために用いられるパラメータを発生させる、請求項1記載の方法において、

前記入力信号及び前記キーの桁が、バイトに集合化され、

前記第1のアルゴリズムが、入力信号及びキーの桁のバイトの各々の対が互いにそれぞれ加算される高合通過を備えている、

前記方法。

4. 通信システムにおける通信の機密性を強化するために用いられるパラメータを発生させる、請求項3記載の方法において、

少なくともいくつかの加算から得られた値が、その入力及びその出力の間で1：1のマッピングを有する固定参照テーブルから数値を得るために用いられる、

前記方法。

5. 通信システムにおける通信の機密性を強化するために用いられるパラメータを発生させる、請求項4記載の方法において、

前記固定参照テーブルが、前記システム内で通信データを暗号化するための疑似ランダムキーストリームを発生するアルゴリズムにおいて用いる数値を得るためにも用いられる、

前記方法。

6. 通信システムにおける通信の機密性を強化するために用いられるパラメータを発生させる、請求項1記載の方法において、

前記入力信号の桁を第2の集合に構成する段階と、

前記入力信号の第2の集合と前記永久及びローリングキーの桁から、第2のアルゴリズムに従って、第2の出力値を計算する段階と、

前記第2の出力値を含む連続的に構成した桁のブロックを、次の特定の時刻に該特定の移動局と関連する新たなローリングキーを含む、前記システム内で用いるための選択されたパラメータに割り当てる段階と、

をさらに含んでいる前記方法。

7. 通信システムにおける通信の機密性を強化するために用いられるパラメータを発生させる、請求項6記載の方法において、

前記第2の出力値を含む連続的に構成した桁のブロックを前記システム内で用いるための選択さ

れたパラメータに割り当てる段階が、前記システム内で通信データを暗号化するための疑似ランダムビットのキーストリームを計算するために秘密キーを使用することをも含んでいる、

前記方法。

8. 通信システムにおける通信の機密性を強化するために用いられるパラメータを発生させる、請求項6記載の方法において、

前記入力信号及び前記キーの桁が、バイトに集合化され、

前記第1及び第2のアルゴリズムが、入力信号及びキーの桁のバイトの各々の対が互いにそれぞれ加算される混合過程を備えている、

前記方法。

9. 通信システムにおける通信の機密性を強化するために用いられるパラメータを発生させる、請求項1記載の方法において、

前記方法は、前記移動局のホーム交換の制御の下で実行される、

前記方法。

10. 通信システムにおいてアクセスを認証する際に用いられるパラメータを発生させる方法であって、移動局には固有の多数桁永久キーが割り当てられ、可変の多数桁ローリングキーが機密性を高めるために用いられており、前記永久キーと前記ローリングキーの両方は、前記移動局及び該移動局が通信を行うネットワークに配信されており、

該ネットワークからの認証問い合せを表わす信号を含む複数の多数桁入力信号を、前記特定の移動局の多数桁永久キー及びその特定の時刻に前記特定の移動局に関連する該多数桁ローリングキーと共に供給する段階と、

前記入力信号の桁の少なくともいくつかを第1の集合（grouping）に構成する段階と、

前記入力信号の第1の集合と前記永久及びローリングキーの桁から、第1のアルゴリズムに従って、第1の出力値を計算する段階と、

前記第1の出力値の少なくとも一部を含む連続的に構成した桁の集合を、該ネットワークによる認証の問い合せに対して応答するために前記移動局によって用いられる認証応答を含む、前記システム内で用いるための選択されたパラメータに割り当てる段階と、

をさらに含んでいる前記方法。

11. ディジタル通信システムにおいてアクセスを認証する際に用いられるパラメータを発生させる、請求項10記載の方法において、

前記第1の出力値の少なくとも一部を含む連続的に構成した桁の集合を、前記システム内で用いるための選択されたパラメータに割り当てる段階が、該ネットワークによってそれを該移動局に対して認証するための認証信号を使用することをも含んでいる、

前記方法。

12. 通信システムにおいてアクセスを認証する際に用いられるパラメータを発生させる、請求項10記載の方法において、

前記入力信号の桁を第2の集合に構成する段階と、

前記入力信号の第2の集合と前記永久及びローリングキーの桁から、第2のアルゴリズムにしたがって、第2の出力値を計算する段階と、

前記第2の出力値の少なくとも一部を含む連続的に構成した桁のブロックを、前記システム内で通信データを暗号化するための疑似ランダムビットのキーストリームを計算するために用いられる安全キーを含む、前記システム内で用いるための選択されたパラメータに割り当てる段階と、

をさらに含んでいる前記方法。

13. 通信システムにおいてアクセスを認証する際に用いられるパラメータを発生させる、請求項10記載の方法において、

前記第2の出力値の少なくとも一部を含む連続的に構成した桁のブロックを前記システム内で用いるための選択されたパラメータに割り当てる段階が、新たなローリングキーを、次の特定の時刻に該特定の移動局に関連付けることをも含んでいる、

前記方法。

国際調査報告

International Application No PCT/US91/05439

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) *

According to International Patent Classification (IPC) or to both National Classification and IPC

IPC(5): H04L 9/00

US. Cl. 380/44

II. FIELDS SEARCHED

Minimum Documentation Searched †

Classification System	Classification Symbols
US. Cl.	380/21,23,25,43,44,46,47,48,49,50 359/33 375/107,110,112
	375/103,105,107 370/76,60

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched ‡

III. DOCUMENTS CONSIDERED TO BE RELEVANT *

Category *	Citation of Document, ** with indication, where appropriate, of the relevant passages **	Relevant to Claim No. **
A	4,876,740 FLEVIUK ET AL) 24 OCTOBER 1989 SEE FIGURE 2A	1-18
A	4,914,698 (KOTCZIAK ET AL) 03 APRIL 1990 SEE FIGURE 4	1-18
A	4,807,257 (MARRY ET AL) 07 MAY 1989 SEE FIGURE 5	1-18
A	4,548,308 (CRAWFORD) 22 OCTOBER 1985, SEE FIGURE 3	1-18

* Special categories of cited documents: **
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
21 AUGUST 1991	29 AUG 1991
International Searching Authority	Signature of Authorized Officer
ISA/US	TOD SWEET

Form PCT/ISA/210 (second sheet) (May 1986)

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : H04L 9/00 — A1

(11) International Publication Number: WO 92/02087

(43) International Publication Date: 6 February 1992 (06.02.92)

(21) International Application Number: PCT/US91/05078

(22) International Filing Date: 18 July 1991 (18.07.91)

(30) Priority data:
556,890 23 July 1990 (23.07.90) US

(71) Applicant: ERICSSON GE MOBILE COMMUNICATIONS HOLDING INC. [US/US]; 15 East Midland Avenue, Paramus, NY 07652 (US).

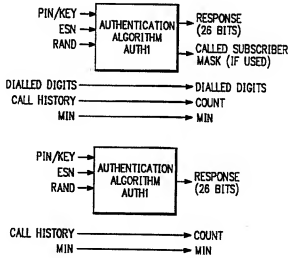
(72) Inventor: DENT, Paul, Wilkinson ; Stehags Prastgard, S-240 36 Stehag (SE).

(74) Agents: CRISMAN, Thomas, L. et al.; Johnson & Gibbs, 900 Jackson Street, Suite 100, Dallas, TX 75202-4499 (US).

(81) Designated States: AU, CA, GB, JP, KR.

Published
With international search report.

(54) Title: AUTHENTICATION SYSTEM FOR DIGITAL CELLULAR COMMUNICATIONS



(57) Abstract

A system for the authentication of mobile stations and base stations in a cellular communications network. The system includes an algorithm which generates not only a key dependent response to a random challenge, but also a temporary conversation key or call variable which may be used to encipher traffic in the network. To protect against clones in the network, the algorithm uses a rolling key which contains historical information. A bilateral authentication procedure may be used to update the rolling key and to generate a new conversation key.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**ES**	Spain	**MG**	Madagascar
AU	Australia	**FI**	Finland	**ML**	Mali
BB	Barbados	**FR**	France	**MN**	Mongolia
BE	Belgium	**GA**	Gabon	**MR**	Mauritania
BF	Burkina Faso	**GB**	United Kingdom	**MW**	Malawi
BG	Bulgaria	**GN**	Guinea	**NL**	Netherlands
BJ	Benin	**GR**	Greece	**NO**	Norway
BR	Brazil	**HU**	Hungary	**PL**	Poland
CA	Canada	**IT**	Italy	**RO**	Romania
CF	Central African Republic	**JP**	Japan	**SD**	Sudan
CG	Congo	**KP**	Democratic People's Republic of Korea	**SE**	Sweden
CH	Switzerland			**SN**	Senegal
CI	Côte d'Ivoire	**KR**	Republic of Korea	**SU**+	Soviet Union
CM	Cameroon	**LI**	Liechtenstein	**TD**	Chad
CS	Czechoslovakia	**LK**	Sri Lanka	**TG**	Togo
DE	Germany	**LU**	Luxembourg	**US**	United States of America
DK	Denmark	**MC**	Monaco		

+ **It is not yet known for which States of the former Soviet Union any designation of the Soviet Union has effect.**

AUTHENTICATION SYSTEM FOR DIGITAL CELLULAR COMMUNICATIONS

CROSS REFERENCE TO RELATED APPLICATIONS

This application contains subject matter related to co-pending U.S. Patent Application Serial No. 556,358, entitled "Encryption System For Digital Cellular Communications"; to co-pending U.S. Patent Application Serial No. 556,102, entitled "Continuous Cipher Synchronization for Cellular Communication System"; and to co-pending U.S. Patent Application Serial No. 556,103, entitled "Resynchronization of Encryption Systems Upon Handoff"; each of which were filed on July 20, 1990 and assigned to the assignee of the present invention. Such applications and the disclosures therein are hereby incorporated by reference herein.

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to digital cellular communication systems, and more particularly, to a method and apparatus for enhancing the security of data communications within such a system.

History of the Prior Art

Cellular radio communications is, perhaps, the fastest growing field in the world-wide telecommunications industry. Although cellular radio communication systems comprise only a small fraction of the telecommunications systems presently in operation, it is widely believed that this fraction will steadily increase and will represent a major portion of the entire telecommunications market in the not too distant future. This belief is grounded in the inherent limitations of conventional telephone communications networks which rely primarily on wire technology to connect subscribers within the network. A standard household or office telephone, for

example, is connected to a wall outlet, or phone jack, by a telephone cord of a certain maximum length. Similarly, wires connect the telephone outlet with a local switching office of the telephone company. A telephone user's movement is thus restricted not only by the length of the telephone cord, but also by the availability of an operative telephone outlet, i.e. an outlet which has been connected with the local switching office. Indeed, the genesis of cellular radio systems can be attributed, in large part, to the desire to overcome these restrictions and to afford the telephone user the freedom to move about or to travel away from his home or office without sacrificing his ability to communicate effectively with others. In a typical cellular radio system, the user, or the user's vehicle, carries a relatively small, wireless device which communicates with a base station and connects the user to other mobile stations in the system and to landline parties in the public switched telephone network (PSTN).

A significant disadvantage of existing cellular radio communication systems is the ease with which analog radio transmissions may be intercepted. In particular, some or all of the communications between the mobile station and the base station may be monitored, without authorization, simply by tuning an appropriate electronic receiver to the frequency or frequencies of the communications. Hence, anyone with access to such a receiver and an interest in eavesdropping can violate the privacy of the communications virtually at will and with total impunity. While there have been efforts to make electronic eavesdropping illegal, the clandestine nature of such activities generally means that most, if not all, instances of eavesdropping will go undetected and, therefore, unpunished and undeterred. The possibility that a competitor or a foe may decide to "tune in" to one's seemingly private telephone conversations has heretofore hindered the proliferation of cellular radio communication systems and, left unchecked, will continue to

threaten the viability of such systems for businesses and government applications.

It has recently become clear that the cellular radio telecommunications systems of the future will be implemented using digital rather than analog technology. The switch to digital is dictated, primarily, by considerations relating to system speed and capacity. A single analog, or voice, radio frequency (RF) channel can accommodate four (4) to six (6) digital, or data, RF channels. Thus, by digitizing speech prior to transmission over the voice channel, the channel capacity and, consequently the overall system capacity, may be increased dramatically without increasing the bandwidth of the voice channel. As a corollary, the system is able to handle a substantially greater number of mobile stations at a significantly lower cost.

Although the switch from analog to digital cellular radio systems ameliorates somewhat the likelihood of breeches in the security of communications between the base station and the mobile station, the risk of electronic eavesdropping is far from eliminated. A digital receiver may be constructed which is capable of decoding the digital signals and generating the original speech. The hardware may be more complicated and the undertaking more expensive than in the case of analog transmission, but the possibility persists that highly personal or sensitive conversations in a digital cellular radio system may be monitored by a third party and potentially used to the detriment of the system users. Moreover, the very possibility of third parties eavesdropping of a telephone conversation eliminates cellular telecommunications as a medium for certain government communications. Certain business users may be equally sensitive to even the possibility of a security breech. Thus, to render cellular systems as viable alternatives to the conventional wireline networks, security of communications must be available on at least some circuits.

Various solutions have been proposed to alleviate the security concerns engendered by radio transmission of confidential data. A known solution, implemented by some existing communication systems, uses cryptoalgorithms to encrypt (scramble) digital data into an unintelligible form prior to transmission. For example, the article entitled "Cloak and Data" by Rick Grehan in BYTE Magazine, dated June 1990 at pages 311-324, for a general discussion of cryptographic systems. In most systems currently available, speech is digitized and processed through an encryption device to produce a communications signal that appears to be random or pseudo-random in nature until it is decrypted at an authorized receiver. The particular algorithm used by the encryption device may be a proprietary algorithm or an algorithm found in the public domain. Further background for such techniques may be found in the article entitled "The Mathematics of Public-Key Cryptography" by Martin E. Hellman in Scientific American dated August 1979 at 146-167.

One technique for the encryption of data relies on "time-of-day" or "frame number" driven keystream generators to produce keystreams of psuedo-random bits which are combined with the data to be encrypted. Such keystream generators may be synchronized to a time of day counter, i.e. hour, minute and second, or to a simple number counter and the encryption and decryption devices may be synchronized by transmitting the current count of the transmitter counter to the receiver in the event one falls out of synchronization with another.

To increase the security of communications in systems utilizing time-of-day or frame number driven keystream generators, the value of each bit in the pseudo-random keystream is preferably made a function of the values of all the key bits in an encryption key. In this manner, a person desiring to descramble the encrypted signal must "crack" or "break" all of the bits of the encryption key which may be in the order of fifty (50) to one hundred (100) bits or more. A keystream of this type is generally produced by

mathematically expanding the encryption key word in accordance with a selected algorithm which incorporates the count of the time-of-day counter. However, if every bit of the encryption key is to influence every bit in the keystream and if the keystream is to be added to the data stream bits on a one-to-one basis, the required number of key word expansion computations per second is enormous and can readily exceed the real time computational capability of the system. The co-pending application entitled "Encryption System for Digital Cellular Communications", referred to above, achieves such expansion of the keystream with conventional microprocessors and at conventional microprocessor speeds.

The use of an encryption key to generate a pseudo-random keystream which is a complex function of all the key bits is a very useful tool for securing digital communications. Other tools may include arrangements for ensuring that the secret key assigned to each mobile station (the permanent key) is never directly used outside of the home network, i.e., the normal service and billing area of the mobile station. Instead, the permanent key is used to generate other bits (the security key) which are used for enciphering a particular call and which may be transmitted from the home network to a visited network, i.e., an area other than the normal billing area into which the mobile station has roamed. Such arrangements reduce the risk of unauthorized disclosure of the permanent secret key to a third party which may use that key to defeat the encryption process.

Yet another tool for securing communications in a digital cellular system is the authentication of mobile stations at registration, call initiation or call reception. Authentication may be simply viewed as the process of confirming the identity of the mobile station. Both authentication and encryption require communication between the visited network and the home network, where the mobile station has a permanent registration, in order to obtain

mobile-specific information such as the security key used for encryption. According to the present invention, the functions of authentication and encryption are linked so that a single inter-network transaction establishes both functions. As described in detail hereafter, the present invention achieves such integration by generating, in the same transaction, not only a key-dependent response (RESP) to a random challenge (RAND), but also the security key (S-key) used to encipher user traffic.

In the American Digital Cellular (ADC) system currently under development, only the air interface is directly specified. Nevertheless, the specification of desirable security functions within the ADC system, e.g., authentication and encryption, can indirectly determine the network security architecture. With respect to authentication, the architecture options relate to whether the authentication algorithm should be executed in the home network or, alternatively, in the visited network. A choice between the two options is necessary for the defintion of a suitable algorithm because the possible input parameters to the algorithm which are available in the home network may not necessarily be the same as those which are available in the visited network. As explained hereafter, the present invention takes account of the significant security benefits which attach to the execution of the authentication algorithm in the home network.

A serious problem in existing cellular systems may be referred to as the "false mobile station" syndrome. Heretofore, it has been possible to copy the entire memory contents of a mobile station and to use that information to manufacture clones which can demand and receive service from the network. One proposed solution is to provide each authorized mobile station with a specific authentication module, or smart card, which has write-only access for the permanent key. This solution, however, renders the mobile station more complex and more expensive. The present invention includes a "rolling key" which provides a more

cost effective safeguard against the threat of false mobile stations. In addition, to meet the threat of a "false base station" in the network, the present invention includes a bilateral authentication procedure which may be used when the rolling key is updated. This two-way authentication procedure enhances security and permits bilateral authentication to be performed on the dedicated traffic channels of the system at any time during a call. Each authentication step may be performed at the option of the network operator, but must be performed at least once after the active presence of a mobile station is first detected within a network so as to generate an S-key for the first call.

A mobile station may occassionaly roam into a small, isolated visited network which lacks the communications links with the home network needed to support authentication and encryption in accordance with the general system of the present invention. Such a visited network may choose to accept a call or registration from the mobile station without performing authentication and to indicate by means of a bit in the traffic channel definition that the mobile identification number (MIN) of the mobile station may be used as a default S-key.

The system of the present invention will be set forth below in connection with an overall digital cellular system and a system for generating a pseudo-random keystream for use in enciphering traffic data in the cellular system. Where appropriate or useful for purposes of background and/or comparison, reference will be made to the EIA/TIA Interim Standard, "Cellular System Dual-Mode Mobile Station-Base Station Compatibility Standard", IS-54, May 1990, published by the Electronic Industries Association, 2001 Pennsylvania Ave., N.W., Washington, D.C. 20006 (hereinafter referred to as "IS-54" and hereby incorporated by reference herein).

SUMMARY OF THE INVENTION

In one aspect the system of the invention includes the generation of a plurality of parameters for use in enhancing the security of communication in a digital cellular communications system in which each mobile station is assigned a unique multi-digit secret permanent key and in which a periodically changed multi-digit rolling key is employed for increased security. Both the permanent key and the rolling key are stored in each mobile station and the home network of the mobile. A plurality of multi-digit input signals are used which include a signal representative of a random authentication inquiry from a visited network and a signal representative of a particular mobile station along with the multi-digit permanent key of the particular mobile station and the multi-digit rolling key associated with the particular mobile at that particular time.

The digits of the input signals are arranged in a first grouping and from that grouping of input signals and the permanent and rolling key digits a first output value is calculated in accordance with a first algorithm. Sequentially arranged blocks of digits comprising said first output value are assigned to selected parameters for use within the system, including, an authentication response to be used by the mobile station to reply to the authentication inquiry by the visited network and an authentication signal to be used by the visited network to authenticate it to the mobile station. The digits of the input signals are then arranged in a second grouping and from that grouping of input signals and the permanent and rolling key digits a second output value is calculated in accordance with a second algorithm. Sequentially arranged blocks of digits comprising said second output value are assigned to selected parameters for use within said system, including, a security key to be used to calculating a keystream of pseuso-random bits for enciphering communications data within the system and a new rolling key to be associated with the particular mobile at a next particular time.

In another aspect of the invention, certain random numbers used in the first and second algorithms are obtained from a look-up table which is also used to obtain random numbers used in an algorithm for calculating a pseudo-random bit stream for enciphering communications data within the system.

In still another aspect of the invention, there is included a system for implementing a digital cellular communications system which includes communications traffic encryption along with bilateral authentication and encryption key generation.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be better understood and its numerous objects and advantages will become apparent to those skilled in the art by reference to the following drawings in which:

FIG. 1 is a pictorial representation of a cellular radio communications system including a mobile switching center, a plurality of base stations and a plurality of mobile stations;

FIG. 2 is a schematic block diagram of mobile station equipment used in accordance with one embodiment of the system of the present invention;

FIG. 3 is a schematic block diagram of base station equipment used in accordance with one embodiment of the system of the present invention;

FIG. 4 is a schematic block diagram of a prior art keystream generator;

FIG. 5 is a schematic block diagram of a keystream generator circuit of an encryption system constructed in accordance with the present invention;

FIG. 6 is a partial schematic block diagram of a second expansion stage of the keystream generator shown in FIG. 5.;

FIG. 7 is a pictorial representation of an authentication algorithm according to a known standard;

FIG. 8 is a pictorial representation of an authentication algorithm according to the present invention;

FIG. 9 is a pictoral representation of a mobile cellular system which uses the authentication algorithm and encryption technique of the present invention;

FIG. 10 is a schematic block diagram of the mixing process used in the authentication algorithm of the present invention; and

FIG. 11 is a schematic block diagram of a building block or mixing cell of the mixing process shown in FIG. 10.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Digital Cellular System

Referring first to FIG. 1, there is illustrated therein a conventional cellular radio communications system of a type to which the present invention generally pertains. In FIG. 1, an arbitrary geographic area may be seen divided into a plurality of contiguous radio coverage areas, or cells, C1-C10. While the system of FIG. 1 is shown to include only 10 cells, it should be clearly understood that, in practice, the number of cells may be much larger.

Associated with and located within each of the cells C1-C10 is a base station designated as a corresponding one of a plurality of base stations B1-B10. Each of the base stations B1-B10 includes a transmitter, a receiver and controller as is well known in the art. In FIG. 1, the base stations B1-B10 are located at the center of the cells C1-C10, respectively, and are equipped with omni-directional antennas. However, in other configurations of the cellular radio system, the base stations B1-B10 may be located near the periphery, or otherwise away from the centers of the cells C1-C10 and may illuminate the cells C1-C10 with radio signals either omni-directionally or directionally. Therefore, the representation of the cellular radio system of FIG. 1 is for purposes of illustration only and is not intended as a limitation on the possible implementations of the cellular radio system.

With continuing reference to FIG. 1, a plurality of mobile stations M1-M10 may be found within the cells C1-C10. Again, only ten mobile stations are shown in FIG. 1 but it should be understood that the actual number of mobile stations may be much larger in practice and will invariably exceed the number of base stations. Moreover, while none of the mobile stations M1-M10 may be found in some of the cells C1-C10, the presence or absence of the mobile stations M1-M10 in any particular one of the cells C1-C10 should be understood to depend, in practice, on the individual desires of each of the mobile stations M1-M10 who may roam from one location in a cell to another or from one cell to an adjacent or neighboring cell.

Each of the mobile stations M1-M10 is capable of initiating or receiving a telephone call through one or more of the base stations B1-B10 and a mobile switching center MSC. The mobile switching center MSC is connected by communications links, e.g. cables, to each of the illustrative base stations B1-B10 and to the fixed public switching telephone network (PSTN), not shown, or a similar fixed network which may include an integrated system digital network (ISDN) facility. The relevant connections between the mobile switching center MSC and the base stations B1-B10, or between the mobile switching center MSC and the PSTN or ISDN, are not completely shown in FIG. 1 but are well known to those of ordinary skill in the art. Similarly, it is also known to include more than one mobile switching center in a cellular radio system and to connect each additional mobile switching center to a different group of base stations and to other mobile switching centers via cable or radio links.

Each of the cells C1-C10 is allocated a plurality of voice or speech channels and at least one access or control channel. The control channel is used to control or supervise the operation of mobile stations by means of information transmitted to and received from those units. Such information may include incoming call signals, outgoing

call signals, page signals, page response signals, location registration signals, voice channel assignments, maintenance instructions and "handoff" instructions as a mobile station travels out of the radio coverage of one cell and into the radio coverage of another cell. The control or voice channels may operate either in an analog or a digital mode or a combination thereof. In the digital mode, analog messages, such as voice or control signals, are converted to digital signal representations prior to transmission over the RF channel. Purely data messages, such as those generated by computers or by digitized voice devices, may be formatted and transmitted directly over a digital channel.

In a cellular radio system using time division multiplexing (TDM), a plurality of digital channels may share a common RF channel. The RF channel is divided into a series of "time slots", each containing a burst of information from a different data source and separated by guard time from one another, and the time slots are grouped into "frames" as is well known in the art. The number of time slots per frame varies depending on the bandwidth of the digital channels sought to be accommodated by the RF channel. The frame may, for example, consist of three (3) time slots, each of which is allocated to a digital channel. Thus, the RF channel will accommodate three digital channels. In one embodiment of the present invention discussed herein, a frame is designated to comprise three time slots. However, the teachings of the present invention should be clearly understood to be equally applicable to a cellular radio system utilizing any number of time slots per frame.

Mobile Station

Referring next to FIG. 2, there is shown therein a schematic block diagram of the mobile station equipment which are used in accordance with one embodiment of the present invention. The equipment illustrated in FIG. 2 may be used for communication over digital channels. A voice signal detected by a microphone 100 and destined for

transmission by the mobile station is provided as input to a speech coder 101 which converts the analog voice signal into a digital data bit stream. The data bit stream is then divided into data packets or messages in accordance with the time division multiple access (TDMA) technique of digital communications. A fast associated control channel (FACCH) generator 102 exchanges control or supervisory messages with a base station in the cellular radio system. The conventional FACCH generator operates in a "blank and burst" fashion whereby a user frame of data is muted and the control message generated by the FACCH generator 102 is transmitted instead at a fast rate.

In contrast to the blank and burst operation of the FACCH generator 102, a slow associated control channel (SACCH) generator 103 continuously exchanges control messages with the base station. The output of the SACCH generator is assigned a fixed length byte, e.g. 12 bits, and included as a part of each time slot in the message train (frames). Channel coders 104, 105, 106 are connected to the speech coder 101, FACCH generator 102 and SACCH generator 103, respectively. Each of the channel coders 104, 105, 106 performs error detection and recovery by manipulating incoming data using the techniques of convolutional encoding, which protects important data bits in the speech code, and cyclic redundancy check (CRC), wherein the most significant bits in the speech coder frame, e.g., 12 bits, are used for computing a 7 bit error check.

Referring again to FIG. 2, the channel coders 104, 105 are connected to a multiplexer 107 which is used for time division multiplexing of the digitized voice messages with the FACCH supervisory messages. The output of the multiplexer 107 is coupled to a 2-burst interleaver 108 which divides each data message to be transmitted by the mobile station (for example, a message containing 260 bits) into two equal but separate parts (each part containing 130 bits) arranged in two consecutive time slots. In this manner, the deteriorative effects of Rayleigh fading may be

significantly reduced. The output of the 2-burst interleaver 108 is provided as input to a modulo-2 adder 109 where the data to be transmitted is ciphered on a bit-by-bit basis by logical modulo-2 addition with a pseudo-random keystream which is generated in accordance with the system of the present invention described below.

The output of the channel coder 106 is provided as input to a 22-burst interleaver 110. The 22-burst interleaver 110 divides the SACCH data into 22 consecutive time slots, each occupied by a byte consisting of 12 bits of control information. The interleaved SACCH data forms one of the inputs to a burst generator 111. Another input to the burst generator 111 is provided by the output of the modulo-2 adder 109. The burst generator 111 produces "message bursts" of data, each consisting of a time slot identifier (TI), a digital voice color code (DVCC), control or supervisory information and the data to be transmitted, as further explained below.

Transmitted in each of the time slots in a frame is a time slot identifier (TI), which is used for time slot identification and receiver synchronization, and a digital voice color code (DVCC), which ensures that the proper RF channel is being decoded. In the exemplary frame of the present invention, a set of three different 28-bit TIs is defined, one for each time slot while an identical 8-bit DVCC is transmitted in each of the three time slots. The TI and DVCC are provided in the mobile station by a sync word/DVCC generator 112 connected to the burst generator 111 as shown in FIG. 2. The burst generator 111 combines the outputs of the modulo-2 adder 109, the 22-burst interleaver 110 and the sync word/DVCC generator 112 to produce a series of message bursts, each comprised of data (260 bits), SACCH information (12 bits), TI (28 bits), coded DVCC (12 bits) and 12 delimiter bits for a total of 324 bits which are integrated according to the time slot format specified by the EIA/TIA IS-54 standard.

Each of the message bursts is transmitted in one of the three time slots included in a frame as discussed hereinabove. The burst generator 111 is connected to an equalizer 113 which provides the timing needed to synchronize the transmission of one time slot with the transmission of the other two time slots. The equalizer 113 detects timing signals sent from the base station (master) to the mobile station (slave) and synchronizes the burst generator 111 accordingly. The equalizer 113 may also be used for checking the values of the TI and the DVCC. The burst generator 111 is also connected to a 20ms frame counter 114 which is used to update a ciphering code that is applied by the mobile station every 20ms, i.e., once for every transmitted frame. The ciphering code is generated by a ciphering unit 115 with the use of a mathematical algorithm and under the control of a key 116 which is unique to each mobile station. The algorithm may be used to generate a pseudo-random keystream in accordance with the present invention and as discussed further below.

The message bursts produced by the burst generator 110 are provided as input to an RF modulator 117. The RF modulator 117 is used for modulating a carrier frequency according to the /4-DQPSK technique (/4 shifted, differentially encoded quadrature phase shift key). The use of this technique implies that the information to be transmitted by the mobile station is differentially encoded, i.e., two bit symbols are transmitted as 4 possible changes in phase: + or - /4 and + or - 3 /3. The carrier frequency for the selected transmitting channel is supplied to the RF modulator 117 by a transmitting frequency synthesizer 118. The burst modulated carrier signal output of the RF modulator 117 is amplified by a power amplifier 119 and then transmitted to the base station through an antenna 120.

The mobile station receives burst modulated signals from the base station through an antenna 121 connected to a receiver 122. A receiver carrier frequency for the selected

receiving channel is generated by a receiving frequency synthesizer 123 and supplied to a an RF demodulator 124. The RF demodulator 124 is used to demodulate the received carrier signal into an intermediate frequency signal. The intermediate frequency signal is then demodulated further by an IF demodulator 125 which recovers the original digital information as it existed prior to /4-DQPSK modulation. The digital information is then passed through the equalizer 113 to a symbol detector 126 which converts the two-bit symbol format of the digital data provided by the equalizer 114 to a single bit data stream.

The symbol detector 126 produces two distinct outputs: a first output, comprised of digitized speech data and FACCH data, and a second output, comprised of SACCH data. The first output is supplied to a modulo-2 adder 127 which is connected to a 2-burst deinterleaver 128. The modulo-2 adder 127 is connected to the ciphering unit 115 and is used to decipher the4 encrypted transmitted data by subtracting on a bit-by-bit basis the same pseudo-random keystream used by the transmitter in the base station encrypt the data and which is generated in accordance with the teachings of the present invention set forth below. The modulo-2 adder 127 and the 2-burst deinterleaver 128 reconstruct the speech/FACCH data by assembling and rearranging information derived from two consecutive frames of the digital data. The 2-burst deinterleaver 128 is coupled to two channel decoders 129, 130 which decode the convolutionally encoded speech/FACCH data using the reverse process of coding and check the cyclic redundancy check (CRC) bits to determine if any error has occurred. The channel decoders 129, 130 detect distinctions between the speech data on the one hand, and any FACCH data on the other, and route the speech data and the FACCH data to a speech decoder 131 and an FACCH detector 132, respectively. The speech decoder 131 processes the speech data supplied by the channel decoder 129 in accordance with a speech coder algorithm, e.g. VSELP, and generates an analog signal representative of the speech

signal transmitted by the base station and received by the mobile station. A filtering technique may then be used to enhance the quality of the analog signal prior to broadcast by a speaker 133. Any FACCH messages detected by the FACCH detector 132 are forwarded to a microprocessor 134.

The second output of the symbol detector 126 (SACCH data) is supplied to a 22-burst deinterleaver 135. The 22-burst interleaver 135 reassembles and rearranges the SACCH data which is spread over 22 consecutive frames. The output of the 22-burst deinterleaver 135 is provided as input to a channel decoder 136. FACCH messages are detected by an SACCH detector 137 and the control information is transferred to the microprocessor 134.

The microprocessor 134 controls the activities of the mobile station and communications between the mobile station and the base station. Decisions are made by the microprocessor 134 in accordance with messages received from the base station and measurements performed by the mobile station. The microprocessor 134 is also provided with a terminal keyboard input and display output unit 138. The keyboard and display unit 138 allows the mobile station user to exchange information with the base station.

Base Station

Referring next to FIG. 3, there is shown a schematic block diagram of the base station equipment which are used in accordance with the present invention. A comparison of the mobile station equipment shown in FIG. 2 with the base station equipment shown in FIG. 3 demonstrates that much of the equipment used by the mobile station and the base station are substantially identical in construction and function. Such identical equipment are, for the sake of convenience and consistency, designated with the same reference numerals in FIG. 3 as those used in connection with FIG. 2, but are differentiated by the addition of a prime (') in FIG. 3.

There are, however, some minor differences between the mobile station and the base station equipment. For

instance, the base station has, not just one but, two receiving antennas 121'. Associated with each of the receiving antennas 121' are a receiver 122', an RF demodulator 124', and an IF demodulator 125'. Furthermore, the base station includes a programmable frequency combiner 118A' which is connected to a transmitting frequency synthesizer 118'. The frequency combiner 118A' and the transmitting frequency synthesizer 118' carry out the selection of the RF channels to be used by the base station according to the applicable cellular frequency reuse plan. The base station, however, does not include a user keyboard and display unit similar to the user keyboard and display unit 138 present in the mobile station. It does however include a signal level meter 100' connected to measure the signal received from each of the two receivers 122' and to provide an output to the microprocessor 134'. Other differences in equipment between the mobile station the base station may exist which are well known in the art.

The discussion thus far has focused on the operational environment of the system of the present invention. A specific description of particular embodiments of the present invention are set forth below. As disclosed above and used hereinafter, the term "keystream" means a pseudo-random sequence of binary bits or blocks of bits used to encipher a digitally encoded message or data signal prior to transmission or storage in a medium which is susceptible to unauthorized access, e.g., an RF channel. A "keystream generator" means a device which generates a keystream by processing a secret key comprised of a plurality of bits. Encryption may be simply performed by a modulo-2 addition of the keystream to the data to be encrypted. Similarly, decryption is performed by a modulo-2 subtraction of an identical copy of the keystream from the encrypted data.

Keystream Generation

Generally speaking, the keystream generator provides a mechanism, represented by elements 115 and 115' of Figs. 2 and 3, respectively, for expanding a relatively small number

of secret bits, i.e., the secret key, represented by elements 116 and 116', into a much larger number of keystream bits which are then used to encrypt data messages prior to transmission (or storage). To decrypt an encoded message, the receiver must "know" the index to the keystream bits used to encrypt the message. In other words, the receiver must not only have the same keystream generator and generate the same keystream bits as the transmitter, but also, the receiver keystream generator must be operated in synchronism with the transmitter keystream generator if the message is to be properly decoded. Synchronization is normally achieved by periodically transmitting from the encoding system to the decoding system the contents of every internal memory device, such as bit, block or message counters, which participate in the generation of the keystream bits. Synchronization may be simplified, however, by using arithmetic bit block counters, such as binary counters, and incrementing those counters by a certain amount each time a new block of keystream bits is produced. Such counters may form a part of a real-time, i.e. hours, minutes and seconds, clock chain. A keystream generator relying on the latter type of counters is known as the "time-of-day" driven keystream generator to which reference was made hereinabove.

It should be noted that the precise method used for bit-by-bit or block-by-block advancing of the keystream generator, and the particular method used for synchronizing the sending circuit with the receiving circuit, are the subject of co-pending patent application serial No. _____, entitled "Continuous Cipher Synchronization for Cellular Communication System", as mentioned above. The system of the present invention, as hereinafter described in detail, is directed to the efficient implementation of an effective encryption system which may be used, for example, to secure digital communication over RF channels in a cellular telecommunications system. The encryption system includes a keystream generator which produces a high number of

keystream bits per second by performing a large number of boolean operations per second on a plurality of key bits contained in a secret key. The keystream generator of the present invention may be implemented with an integrated circuit having a simple microprocessor architecture.

Referring now to FIG. 4, a schematic block diagram of a prior art keystream generator may now be seen. An optional block counter 201 provides a first multi-bit input to a combinatorial logic circuit 202. A plurality of one-bit memory elements, or flip-flops, m1, m2, m3...mn provides a second multi-bit input to the combinatorial logic circuit 202. A portion of the output of the combinatorial logic circuit 202, consisting of one-bit outputs d1, d2, d3...dn, is fed back to the flip-flops m1-mn. The outputs d1-dn become the next state of the flip-flops m1-mn, respectively, after each clock pulse in a series of bit clock input pulses 203 supplied to the flip-flops m1-mn. By suitable construction of the combinatorial logic circuit 202, the flip-flops m1-mn may be arranged to form a straight binary counter, a linear feedback shift register executing a maximum length sequence, or any other form of linear or non-linear sequential counters. In any event, each of the states of the flip-flops m1-mn and the state of the block counter 201 at the receiver end must be made equal to the states of the corresponding elements at the transmitter end. A reset or synchronization mechanism 204 is used to synchronize the receiver with the transmitter.

With continuing reference to FIG. 4, a plurality of secret key bits k1, k2, k3...kn, forms a third multi-bit input to the combinatorial logic circuit 202. The number n of secret key bits is usually in the region of a hundred bits plus or minus (+/-) a factor of 2. It is desirable that each of the secret key bits k1-kn should, at a minimum, have the potential of affecting each of the bits in the keystream. Otherwise, an eavesdropper would need to break only a small subset of the secret key bits k1-kn in order to decipher and monitor the encrypted data. The risk of

unauthorized interception, however, may be considerably reduced if the value (logical state) of each bit in the keystream is made to depend not only on the value of a particular secret key bit, but also on the value of all other secret key bits as well as the state of the block counter 201 and other internal memory states. Heretofore, the establishment of such a dependence would have entailed a prohibitive number of boolean operations. Assume, for example, that the secret key is composed of one hundred (100) secret key bits. If each of these secret key bits is to influence every bit in the keystream, a total of one hundred (100) combinatorial operations per keystream bit would be required. Thus, to produce ten thousand (10,000) keystream bits, a total of one million (1,000,000) combinatorial operations would be required and the number would be even greater if each keystream bit was also made to depend on on one or more internal memory states. One of the objectives of the present invention is to significantly reduce the required number of combinatorial operations per keystream bit while maintaining the dependence of each keystream bit on every one of the secret key bits.

The production of many thousands of pseudo-random keystream bits from, for example, fifty (50) to one hundred (100) secret key bits may be viewed as a multi-stage expansion process. A plurality of expansion stages are cascaded together, each having a successively smaller expansion ratio. Expansion by the first stage is performed less frequently than by subsequent stages in order to minimize the number of required logical (boolean) operations per keystream bit. Additionally, the first expansion stage is constructed to provide a plurality of output bits which is highly dependent on the secret key bits, further reducing the number of logical operations which must be performed by the subsequent stages.

Referring next to FIG. 5, there is shown a schematic block diagram of a keystream generator system. A plurality of security key bits k1, k2, k3... are provided as input to

a first stage expansion 205. The security key bits may be obtained from the permanent key bits by an authentication algorithm as set forth in further detail below. The security key bits k1, k2, k3... input may include some, but preferably all, of the security key bits k1, k2, k3...kn, hereinafter sometimes referred to as "secret" key bits. Additional, or optional, inputs to the first stage expansion 205 may include the outputs of a message counter, a block counter, a date-time stamp representing the time or block count number at the start of a frame, or other variable outputs which may be synchronized by the sender and receiver. Any internal memory output which varies slowly with time may be used as an input to the first stage expansion 205. A slow changing input is desired because the first stage expansion 205 should be performed infrequently, e.g., once per message.

The first stage expansion 205 generates an expanded output which is considerably larger in size than the number of secret key bits k1, k2, k3... The expanded output is stored in a memory device 206 which is accessed by a combinatorial logic circuit 207. The combinatorial logic 207 performs a second stage expansion as more fully set forth below. The output of a counter or register 208 forms an input to the combinatorial logic 207. The register 208 is initialized to a new starting state prior to the generation of each block of keystream bits. An initial value generator 209 provides the starting state for the register 208. The starting state, which will be different for each particular block of keystream bits, is a function of the block number of the particular block and, possibly, also a function of some subset of the secret key bits k1-kn.

A first output 210 of the combinatorial logic 207 is fed back to the register 208. The output 210 becomes the new state of the register 208 after each cycle of operation. A second output 211 of the combinatorial logic 207 forms the keystream bits which are to be mixed with the data stream as shown in Figs. 2 and 3, above. The number of keystream bits

produced per cycle at the output 211 may be any multiple of 2, i.e, 8, 16, 32, 56, etc. Such bits are collectively referred to as a "keyword". Some or all of the keywords produced at the output 211 prior to reinitialization of the register 208 are grouped into a keyblock 212. The keyblock 212 may, for example, consist of all the keywords produced in every cycle, or in every other cycle, preceding reinitialization of the register 208.

It will be appreciated by those skilled in the art that a conventional implementation of the keystream generator system depicted in FIG. 5 and discussed above might require a host of complex combinatorial logic circuits which, if realized separately by interconnecting a plurality of logic gates, i.e, AND, OR etc., would amount to a large and costly chip, useful only for a very specific application. An arithmetic and logic unit (ALU), on the other hand, is a standard component of a variety of small, low-cost and multi-purpose microprocessors. The present invention provides a means for realizing all of the required combinatorial logic functions with the use of such an ALU.

The conventional ALU, operating under the control of a program, can perform the combinatorial functions ADD, SUBTRACT, BITWISE EXCLUSIVE OR, AND, OR between any two 8-bit or 16-bit binary words. If the ALU is used to sequentially implement all of the boolean functions required in the device of Fig. 5, the ALU operating speed, measured in terms of the number of complete cycles per second that may be executed, would be substantially reduced. The multi-stage expansion used in the present system, however, prevents such excessive reduction of ALU speed by minimizing the number of program instructions, i.e., instances of ALU utilization, per cycle for the most frequently executed combinatorial logic 207 through the infrequently periodic calculation of a large number of key-dependent functions in the first stage expansion 205. By the word "large" in the preceding sentence, is meant, for example, an order of magnitude larger than the number n of secret key bits.

Once the register 208 is initialized with a starting value, the combinatorial logic 207 will generate a stream of keywords at the output 211 and will continue to generate additional keywords each time the register 208 is reloaded with the feedback value at the output 210. Difficulties may arise, however, which can undermine the integrity of the keyword generation process. If, for example, the contents of the register 208 ever return to their initial value, the sequence of the keywords generated theretofore will repeat again. Similarity, if the contents of the register 208 return to a value (not necessarily the initial value) previously encountered in the generation of the current keyblock, the system is said to be "short cycling". For reasons alluded to earlier, e.g., the ease of unauthorized deciphering, it is undesirable that the sequence of keywords should begin to repeat, or that short cycling should occur, within the generation of a single keyblock. Moreover, if the contents of the register 208 at some point, say after the m'th keyword is generated, become equal to some value which existed or will exist after the m'th keyword during the generation of another keyblock, the two keyblocks will, from that point on, be identical--also an undesirable occurrence.

Hence, the combinatorial logic 207 and the associated register 208 (the "combinatorial logic/register combination"), when operated successively a number of times, should (i) not produce cycles shorter than the number of keywords per block; and (ii) produce a unique keyword sequence for every unique starting state of the register 208. To meet the latter requirement, no two different starting states should be capable of converging to the same state. Furthermore, both of the foregoing requirements should apply regardless of the contents of the memory 206. As explained in more detail below, the present invention alleviates these concerns and enhances the integrity of the keyword generation process.

When the state transition diagram of the combinatorial logic/register combination has converging forks, the combination may not be run in reverse through such a fork because of the ambiguity about which path to take. Therefore, if a process for operating the combination can be shown to be unambiguous or reversible, it is proof that converging forks do not exist in the state transition diagram. Such a process is described and discussed below.

Referring next to Fig. 6, a partial schematic block diagram of the second expansion stage of the keystream generator shown in FIG. 5 may now be seen. The register 208 of FIG. 5 has been divided into three byte-length registers 208A, 208B, 208C in FIG. 6. The registers 208A, 208B, 208C may be, for example, 8-bit registers. Following initialization of the registers 208A, 208B, and 208C, new state values are calculated from the following formulas:

(1) $A' = A \# [K(B) + K(C)]$

(2) $B' = B \# R(A)$

(3) $C' = C + 1$

where,

A′ is the new state value for the register 208A;

B′ is the new state value for the register 208B;

C′ is the new state value for the register 208C;

A is the current state value for the register 208A;

B is the current state value for the register 208B;

C is the current state value for the register 208C;

\+ means word-length modulo additions, for example, byte wide modulo-256 additions;

\# means + (as defined above) or bitwize EXclusive OR (XOR);

K(B) is the value K located at address B of the memory 206 shown in FIG. 5;

K(C) is the value K located at address C of the memory 206 shown in FIG. 5;

It should be noted that each of the values K stored in the memory 206 has been previously calculated to be a complex function of all the secret keybits by the first stage

expansion 205 shown in FIG. 5. R(A)is the value located at address A in a fixed look-up table R which may be the same tible which is described below in connection with the contents of the S-Box use in the authentication algorithm. Alternatively, the bits of A are supplied as inputs to a combinatorial logic block which will produce an output R. The look-up table R, or alternatively, the combinatorial logic block should provide a number of output bits greater or equal to the word length of A and less or equal to the word length of B. In the case where A and B are both 8-bit bytes, for example, R will also be an 8-bit byte and the look-up table R will contain 256 values.

The value R should have a 1:1 mapping from input to output; that is, each possible state of the input bits should map to a unique output value. This ensures that the R function is reversible which, in turn, ensures that the whole process may be reversed by means of the following relationships:

(1) C = C - 1

(2) B = B ## R′(A)

(3) A = A ## [K(B) + K(C)]

where,

- means word-length modulo subtraction;

means the inverse operation of #, i.e., either- (as defined above) or bitwise XOR; and

R′ is the inverse of the 1:1 look-up table, or the combinatorial logic, R.

This reversibility demonstrates that there are no converging forks in the state transition diagram of the combinatorial logic/register combination and, hence, guarantees that every starting state will produce a unique sequence of keywords. Furthermore, the process guarantees a minimum cycle length, since C is incremented only by 1 and will not return to its initial value until after 2^w iterations, where w is the word length used. For example, if all of the values A, B, C, R and K are 8-bit bytes, the minimum cycle length will be 256. If, upon every iteration

(cycle), a keyword (byte) is extracted, a total of 256 bytes may be extracted without the danger of premature repetition of the sequence. If, on the other hand, the keyword is extracted every other iteration, a total of 128 keywords may be extracted without premature repetition of the sequence. By the word "extracted" in the preceding two sentences, is meant the collection and placement of keywords into a keyblock such as the keyblock 212 in FIG. 5. A particular method of keyword extraction which may be used in the present invention is described immediately below.

In connection with FIG. 6, a process was described for computing the outputs 210 of the combinatorial logic 207 which are fed back to the register 208. Generally speaking, any one of the intermediate quantities A, B or C may be directly extracted and used as a keyword on each iteration. Letting S = (A, B, C) stand for the current state of the combinatorial logic/register combination, the combination will transit through a sequence of states S0, S1, S2, S3, S4, S5, S6, S7... following initialization to S0. If, however, in the computation of a subsequent keyblock the register 208 is initialized, for example, to S2, the resulting sequence S2, S3, S4, S5, S6, S7... will be identical to the first sequence but shifted by two keywords (S0, S1). Therefore, if a value A, B, or C from a state S is directly used as a keyword, such an identity may appear between different keyblocks. To prevent this, the system of the present invention modifies each of the values extracted in accordance with the value's position in the keyblock so that if the same value is extracted to a different keyword position in another block, a different keyword will result. An exemplary method for achieving the latter objective is set forth below.

Let N be the number of keywords in the keyblock currently being computed and S = (A, B, C) be the current state of the register 208 in the iteration during which the keyword N is to be extracted. The value of the keyword W(N) may be calculated as follows:

W(N) = B +' K[A + N]

where,

+ means XOR;

+' means either + (as defined immediately above) or word length-modulo addition.

Other suitable exemplary methods for keyword extraction may include the following:

W(N) = B + K[R(A + N)] or

W(N) = R[A + N] + K[B + N] and so forth.

It is recommended that, to obtain the best cryptographic properties in the system, the values of the keywords extracted should be a function of their respective positions within a keyblock.

Having described an encryption system which generates a large number of complex, key-dependent pseudo-random (PR) bits for use in enciphering data and which may be implemented in a conventional microprocessor, a description of a system which integrates the encryption and authentication functions and improves the overall security of a digital cellular system is set forth immediately below.

Authentication

The process of authentication according to the present invention generally involves the following sequence of steps:

(1) The mobile station identifies itself to the network by sending a mobile identification number (MIN) in unencrypted form so that the network can retrieve information pertaining to that mobile, e.g., security keys, from the location or database in which they are stored.

(2) The network transmits a random challenge signal (RAND) to the mobile.

(3) The mobile station and the network each uses bits of a secret permanent authentication key, known only to the mobile station and the network and never transmitted over the air, in order to compute a response signal (RESP) to the RAND in accordance with a published

algorithm (referred to hereinafter as AUTH1). The RESP generated at the mobile station is transmitted to the network.

(4) The network compares the RESP received from the mobile station with the internally generated version and grants the mobile station access for registration, initiation of a call or reception of a call only if the comparison succeeds.

In IS-54, the MIN is a 34-bit binary word which is derived from the mobile station's 10-digit directory telephone number, i.e., area code and telephone number. See IS-54, §2.3.1 at pp. 78-79. The mobile station stores a 16-bit value in a random challenge memory which represents the last RAND received in a random challange global action message periodically appended to the overhead message train. The mobile station uses these messages to update the random challenge memory. The present value of the RAND is used as an input to the authentication algorithm AUTH1. See IS-54, §2.3.12 at pp. 83-84. Thus, in IS-54, the RAND is transmitted to to the mobile station before the mobile station transmits the MIN and only one RAND is in use for all the mobile stations, including false mobile stations, in the network at any particular time thereby reducing the level of security in the system. Moreover, since the RAND is known to the mobile station in advance, the RESP is precalculated and transmitted to the network along with the MIN. The network, however, could not have precalculated the RESP without receiving the MIN unless the mobile station was previously registered in the network.

The authentication key used in the AUTH1 of the IS-54 system consists of a personal identification number (PIN) which is a secret number managed by the system operator for each subscriber. The IS-54 AUTH1 also uses a factory-set electronic serial number (ESN) which uniquely identifies the mobile station to any cellular system. The RESP computed by the IS-54 AUTH1 depends on: (i) the PIN; (ii) the ESN; and (iii) the dialed digits (for mobile originated calls) or the

MIN (for mobile terminated calls). The RESP transmitted by the mobile station according to IS-54 consists of the output of AUTH1 (AUTHR) (18 bits) together with a random confirmation (RANDC) (8 bits), which depends on RAND, for a total of 26 bits. No cryptological distinction is made between AUTHR and RANDC and each of these values may depend on the values of RAND, PIN, ESN and perhaps the called number. Thus, AUTHR and RANDC may be regarded as merely constituting a 26-bit RESP, the nature of which is determined by the algorithm AUTH1 which is used.

The use of the dialed digits, in accordance with IS-54, to affect the RESP in the case of a mobile originated call set-up has certain undesirable or noteworthy consequences which are listed below:

(1) Since the dialed digits cannot be known to the network in advance, the network cannot precalculate the expected RESP to a given RAND for any particular MIN. Hence, the authentication algorithm AUTH1 cannot be executed until the dialed digits are transmitted from the mobile station to the network possibly delaying call set-up. On the other hand, if the dialed digits are not included, the same mobile station will produce the same RESP for as long as the RAND remains unchanged. In such instance, it is possible to intercept and use the RESP to place a fraudulent call and, thus, to defeat the basic reason for having AUTH1 at all.

(2) Use of the dialed digits as an input to AUTH1 precludes the home network from generating RAND and RESP pairs and sending them to visited networks in advance.

(3) Such use also precludes the advance precalculation of RAND and RESP pairs in general, which may be desirable to save time at call set-up.

(4) Such use implies some assumptions about inter-network, security-related communications and/or the location of the authentication function. In particular, it implies either that the home network transmits the secret key

(and the ESN) to the visited network so that the visited network may perform authentication or, alternatively, that the dialed digits are sent on each call from the visited network to the home network so that the home network may execute authentication. The home network would not normally need to know the called subscriber number in advance.

(5) Since the dialed digits must be transmitted in unencrypted form, according to IS-54, a false mobile station may be able to place a call to the same number and then, through a "flash" or conferenceing procedure, connect to another number of his choice.

(6) In at least one existing network, it has been deemed necessary to introduce Called Subscriber Identity Security, i.e., masking the dialed digits, in order to prevent certain abuses and the definition of AUTH1 should accomodate such required masking.

The system of the present invention addresses all of the concerns listed above by defining an algorithm AUTH1 in which the dialed digits do not affect RESP. Any weakness caused by the exclusion of the dialed digits from AUTH1, for example, the generation of an identical RESP as long as RAND remains unchanged, is compensated for by defining a second, optional, bilateral authentication step which may be available on the traffic channel. Further safeguards are provided by the process of encryption of the traffic data. It should be noted that the present invention may be used without substantially changing the specifications of IS-54.

Regardless of which location, the home network or the visited network, is considered more convenient for executing the authentication algorithm, some exchange of security-related subscriber information between the networks is unavoidable if authentication or encryption is to take place. In the IS-54 authentication procedure where the visited network periodically determines and broadcasts the RAND, if the authentication algorithm is executed in the home network, the visited network must transmit at least MIN

and RAND to the home network in order to receive an RESP and a temporary security encryption key (S-key or call variable). On the other hand, if the authentication algorithm is executed in the visited network, that network must transmit at least MIN to the home network and the home network must, in turn, transmit to the visited network the authentication key, the ESN (if ESN is used in AUTH1) and the permanent encryption key. From a security standpoint, it is undesirable for the home network to release a subscriber's permanent key merely on demand by a visited network. Such keys should constitute the subscriber's long-term security guarantee rather than a short-term call variable. It is, therefore, more desirable that the home network, upon receiving from the visited network the MIN of a visiting mobile station, the RAND broadcast by the visited network and the RESP received by the visited network from the mobile station, generate a short-term (temporary) ciphering key (S-key or call variable) and release the S-key to the visited network only if the RESP is deemed valid.

Execution of the authentication algorithm in the home network allows the authentication algorithm to use the long-term (permanent) secret key, referred to herein as the A-key, which is unique to each mobile station. The A-key is never released outside the home network and never used directly for enciphering but is, instead, used for generating a short-term encryption key, referred to herein as the S-key. The S-key is used only for a limited period of time to be determined by the visited network. If the visited network has already acquired an S-key for a previously registered visiting mobile station, performance of the first authentication step is optional and call set-up may proceed directly to the enciphered traffic channel. Hence, it is not necessary for inter-network exchanges to take place every time a visiting mobile station places a call. If, on the other hand, the visited network decides to request an AUTH1 first authentication step, the mobile station and the home network will use the current RAND of

the visited network to generate a new S-key, with other inputs to the AUTH1 algorithm being unchanged.

Cryptoanalytic Properties of Authentication Algorithms

Referring now to FIG. 7, a pictorial representation of an authentication algorithm according to IS-54 may now be seen. When a call is initiated by the mobile station, the mobile station uses its PIN or authentication key, its ESN, the RAND and the dialed digits to compute a response to RAND in accordance with an authentication algorithm AUTH1. The mobile station then transmits to the network the output of AUTH1 (AUTHR) together with random confirmation (RANDC), the dialed digits, the mobile station's individual call history parameter (COUNT) and the MIN. The consequences of allowing the dialed digits to affect the authentication response (AUTHR and RANDC) in mobile originated calls were discussed above and are deemed undesirable. On the other hand, it was considered desirable to accomodate the possibility of called subscriber identity masking. In the case of mobile terminated calls, little is gained by using MIN to affect the authentication response, since the PIN/key is sufficiently mobile-specific.

Referring now to FIG. 8, a pictorial representation of an authentication algorithm according to the present invention may be seen. Neither the dialed digits in the case of mobile originated calls, nor the MIN in the case of mobile terminated calls, are used as input to AUTH1. Futher, the output of AUTH1 according to the present invention includes not only an authentication response (RESP), but also a called subscriber mask which may be used to mask the dialed digits in the case of a mobile originated call. A particular embodiment of AUTH1 is set forth and explained below.

A mobile station may be borrowed, stolen or legally acquired and its entire memory contents may be copied, including its ESN, secret keys, PIN codes, etc., and used to manufacture a number of clones. The cloning procedure may be quite sophisticated and may include software

modifications which replace physically stored ESN information with electronically stored information so that a number of stored mobile station identities may by cyclically rotated within one false mobile station and used to imitate several genuine mobile stations.

Call numbering has been proposed as a means for enabling the network to identify whether clones exist. In call numbering, a modulo-64 count is kept in the mobile station and is incremented after each call or when commanded by the network. A similar count is also kept in the network. The mobile station transmits its call number to the network at call step-up and the network compares the received call number with the internally generated version. The comparison, however, may fail for one of several reasons:

(1) The mobile station may have failed to update its call count after the last call because of an abnormal termination, such as a power failure.

(2) The mobile station may have updated its call count but the network did not receive confirmation that the mobile station had done so because of an abnormal termination.

(3) A clone mobile station had placed one or more calls and stepped up the network counter.

(4) The mobile station is itself a clone and the "real" mobile station had, meanwhile, stepped up the counter.

Unfortunately, the call counter is too easily modified in either direction for the network to determine which of the preceding conditions has occurred and the network may thus be forced to deny service to the mobile station. To avoid such a drastic result, the mobile subscriber may be given an additional opportunity to manually identify himself or herself to the network by, for example, keying in a short secret number which is not stored in the mobile station memory. The system of the present invention provides another anti-cloning safeguard based on a dynamic "rolling key" which is stored in each of the home network and the

mobile station and which is used along with the permanent secret key for calculating authentication responses and temporary encryption keys. While such rolling keys have been previously used for authentication alone, they have not been employed to produce both authentication and encryption paramenters.

The principle behind the rolling key concept is to require certain historical information in each of the network and the mobile station to match as a means of protection against clones and as an alternative to requiring complex and expensive physical protection of mobile station memories. Specifically, in order for a clone mobile station to gain access to the system, the clone would be required to intercept the entire history of authentication challenges subsequent to the time of copying the then current key state of a genuine mobile station. According to the present invention, authentication is carried out in the home network using a combination of a rolling key, referred to herein as the B-key, which contains historical information, and the permanent secret subscriber key (A-key), which is never used directly in an encryption algorithm but is used only for generating one or more operating security keys. The authentication algorithm of the present system also computes a new value for the rolling key which becomes the current value of the rolling key whenever the mobile station and the home network agree on an update. Such an update may be triggered by a request from the visited network or the home network for execution of a bilateral authentication procedure as further described below.

The rolling key update may be performed at any time during a conversation that the visited network decides to update the call counter in the home network and the mobile station. Before updating its call counter, the home network may request a bilateral authentication of the mobile station. A correct response from the mobile station would then result in a call counter update, a rolling key update and the generation of a new conversation security key (S-

key) which is sent to the visited network for use in subsequent calls. Similarly, the mobile station may update its call counter only if the bilateral authentication procedure verifies that the visited network is in genuine contact with the home network. Upon verification, the mobile station also updates its call counter and rolling key (B-key) and generates a new conversation security key (S-key) for use in subsequent calls served by the same visited network. It may be appreciated that, because the call counter and the rolling key are updated at the same time, a check of the mobile station and the home network call counters may also serve as an indication of whether the mobile station and home network are in the same rolling key state.

Bilateral Authentication

Bilateral authentication, i.e., authentication of both the mobile station and the network, may be distinguished from unilateral authentication in that the authentication information sent in both directions is key-dependent in the former, whereas only the information sent in the direction mobile station to network is key-dependent in the latter. According to the present invention, the RAND signal is used as an input to an authentication algorithm AUTH2 which generates a long RESP signal, part of which is sent from the network to the mobile station to validate the network and the other part is sent by the mobile station to the network to validate the mobile station. For example, the algorithm AUTH2 could compute a RESP from the RAND and then proceed to use the RESP as a new RAND input to the algorithm AUTH2 which then computes a RESPBIS signal. The network transmits the RAND and the RESPBIS to the mobile station which uses the RAND to compute a RESP and a RESPBIS in accordance with the AUTH2. The mobile station will send the internally generated RESP to the network only if the internally generated RESPBIS matches the RESPBIS received from the network. This prevents a false base station from extracting RAND, RESP pairs from the mobile station and the

verification of the mobile station and network identities allows security status updating to proceed at a convenient later point in relative safety.

Enciphering Key (Call Variable or S-Key) Generation

When enciphering of communication is desired in a visited network the ciphering key must be communicated from the home network to the visited network. As mentioned heretofore, it is highly undesirable for the permanent secret subscriber A-keys to circulate between networks on non-specially protected links. Instead, and in accordance with the present invention, the home network never releases the A-key of a given subscriber but only uses the A-key to generate a temporary talk-variable security key (S-key) which is then used to generate a pseudo-random keystream for enciphering a particular call or group of calls. It should be understood that the "secret key" referred to in the earlier discussion of the pseudo-random keystream generation technique of the present invention represents the S-key which is directly used for encryption and not the permanent secret A-key from which the S-key is derived. The S-key is calculated and sent from the home network to the visited network upon receiving a MIN, a RAND and a RESP which are valid.

Since the S-key is calculated at the same time and by the same process as the authentication challenge-response signal (RESP), successful authentication ensures that the network and the mobile station will have the same enciphering key (S-key) and, consequently, the enciphering of user data may begin as soon as authentication has been completed. It may thus be seen that the linkage of authentication and enciphering in the system of the present invention reduces the number of different security-feature combinations that must be identified by the mobile station and the base station from four (4) to two (2).

Input and Output Bit Count

The talk-variable (S-key) may be generated as a by-product of the same authentication algorithm which produces

the RESP and RESPBIS parameters mentioned above. Other desired outputs from such an algorithm may include (i) sufficient bits to mask the called subscriber number; and (ii) the next state of the rolling key (B-key) which replaces the current state if the network has been validated by bilateral authentication and/or the call counter update command has been issued.

By way of example and without any limitation on the teachings of the present invention, the following table illustrates a bit and byte count for the algorithm outputs:

OUTPUT	NO. OF BITS	NO. OF BYTES
RESP	32	4
RESPBIS	32	4
CALLED NO. MASK	64	8
S-key	64	8
NEXT B-key	64	8
TOTAL BITS	256	TOTAL BYTES 32

The following table illustrates a bit and byte count for the algorithm inputs:

INPUT	NO. OF BITS	NO. OF BYTES
A-key	128	16
B-key	64	8
RAND	32	4
ESN	32	4
DIALED DIGITS	0	0
TOTAL BITS	256	TOTAL BYTES 32

The values depicted above have been deliberately rounded up to give an algorithm having a 32-byte input and a 32-byte output. If shorter variables are used, they may be expanded with constants. An algorithm having the above input and output byte counts and which is suitable for fast execution by byte-wide operations in a simple 8-bit microprocessors of the type commonly found in mobile stations, is set forth below in a separate section entitled "Definition of Authentication Algorithm."

General Properties of the Present System of Authentication

The present invention provides two steps of authentication which may be used at the network operator's discretion. The first step has been referred to as AUTH1 in the preceding description. The algorithm set forth in the section entitled Definition of Authentication Algorithm may be used for AUTH1. In such algorithm, the dialed digits do not affect the outputs. The 16-bit RAND broadcast on the control channel is used and included twice to provide a 32-bit input. The algorithm output parameters include the RESP and the MIN which may be sent by the mobile station to the network on the calling channel and the call variable (S-key) which may be used for enciphering user data immediately upon switching to a TDMA traffic channel. An additional output parameter is provided for masking the called subscriber number in the case of mobile originated calls. This parameter may be sent from the home network to the visited network so that the called number can be unmasked.

The second authentication step, referred to as AUTH2 in the preceding description, is a bilateral authentication procedure which may be carried out at the network's discretion once communication has been established on the traffic channel. The purpose of the bilateral authentication step is to trigger a rolling key (B-key) update in both the mobile station and the home network while, at the same time, validating them to each other and, thus, preventing certain forms of false base station attacks on the security of the system. The algorithm for AUTH2 is exactly the same as the algorithm for AUTH1 set forth below in the section entitled Definition of Authentication Algorithm, except that the RAND value is determined by the home network and sent along with a RESPBIS to the visited network and, therefrom, to the mobile station. If the mobile station validates the RESPBIS, the mobile station will send a RESP to the visited network which sends the RESP to the home network. If the home network validates the

RESP, the home network will send to the visited network an S-key which may be used for the next call.

Referring now to FIG. 9, there is shown therein a pictorial representation of a mobile cellular system which uses the authentication algorithm and encryption technique of the present invention. For convenience, only one mobile station, one visited network and one home network are illustrated in FIG. 9 although it should be understood that a number of mobile stations, visited networks and home networks are usually found in practice. The following abbreviations, as seen in FIG. 9, are of the following terms:

A1 and A2:	AUTH1 and AUTH2, respectively
A3:	Encryption technique in accordance with the present invention
IVCD:	Initial Voice Channel Designation
MS:	Mobile Station
VLR:	Visited Network
HLR:	Home Network

In FIG. 9, the visiting network periodically broadcasts a new RAND1 value to all mobile stations within its service area. Each of the mobile stations computes a response RESP1 which is sent along with MIN and the call history parameter COUNT to the visited network (note that in some applications the RESP1, MIN and COUNT may be sent separately). The visited network requests the enciphering key (S-key) for a particular mobile station from the mobile station's home network. The home network compares the received response RESP1 with the parameters it has obtained by applying RAND1, ESN, A-key and B-key to the authentication algorithm A1 and determines whether the mobile station is genuine whereupon the home network releases a temporary enciphering key (S-key) to the visited network. If the visited network does not receive an enciphering key, the visited network may deny service to the mobile station.

If the visited network grants access and assigns a TDMA channel (or a control channel in some applications) to the

mobile station, the parameters defining that channel, i.e., frequency, timeslot and DVCC, are sent from the visited network to the mobile station which tunes to the allocated traffic (or control) channel. Therafter, the visited network and the mobile station may communicate in the enciphered mode using the S-key. The visited network sends its frame counter value over the unencrypted SACCH and also sends frame count synchronization messages in a fixed number of unencrypted FACCH messages as described in the related co-pending patent application entitled "Continuous Cipher Synchronization for Cellular Communication System", referred to and incorporated by reference above. Further exchanges of FACCH signalling or traffic may take place in the enciphered mode.

Bilateral Authentication and Rolling Key Update

Once the mobile station and the base station have established communication on the traffic channel, the visited network may, at any time, request the execution of bilateral authentication and rolling key and call counter update by sending to the mobile station a RAND2 and a RESP3 received from the home network. The mobile station uses the RAND2, ESN, A-key and B-key in A2 to generate the expected RESP3 and RESP2. IF the internally generated RESP3 agrees with the received RESP3, the mobile station sends a RESP2 to the visited network. The visited network sends RESP2 to the home network and, if the home network's internally generated RESP2 agrees with the received RESP2, a newly calculated call variable S-key will be sent from the home network to the visited network. The visited network stores the S-key for use in future calls involving the visiting mobile station. The present call continues to be enciphered with the old S-key. Upon handover or call termination, the new S-key will come into use.

Definition of Authentication Algorithm

Summary of Description

The authentication algorithm of the present invention may be used for both authentication on the calling channel

(AUTH1) and bilateral authentication on the traffic channel (AUTH2). Exemplary coding of the algorithm is given for some common microprocessor implementations. In the description which follows, certain byte counts have been chosen for the input and output variables of the algorithm. It should be clearly understood, however, that such byte counts are exemplary only and are not intended and should not be construed as a limitation on the applicability of the present authentication algorithm.

Input and Output Variables of Algorithm

The algorithm of the system of the present invention uses a total of 32 bytes of input signals and generates 32 bytes of output parameters. This is achieved by two applications of an algorithm which uses 16 bytes of input variables and generates 16 bytes of output variables. The input variables are:

RAND: Provision is made for up to 4 bytes] NON-SECRET

ESN: Provision is made for up to 4 bytes] VARIABLES

Ka: 16 bytes of the permanent key (A-key)] SECRET

Kb: 8 bytes of the rolling key (B-key)] VARIABLES

The 32 output bytes are designated for use withing the system as the following parameters:

0-3 : Authentication response (RESP)

4-7 : RESPBIS (needed for bilateral authentication)

8-15 : Called subscriber number mask (if used)

16-23: Next Kb if key update occurs

24-31: Talk variable for enciphering this call (S-key)

The 32 bytes of input to the algorithm are split into groups of 16 bytes which are then used in the first application of the algorithm to produce a first 16 bytes of output (bytes 0-15). The 32 bytes of input are then split in a different way and used in the second application of the algorithm to produce a second 16 bytes of output (bytes 16-31).

General Structure of the Algorithm

The present algorithm (code) is adapted for very efficient and fast execution on simple microprocessors of the type used in cellular radio telephones. Recursive use of a small inner code loop serves to confine the code within a 100-byte region. The outer loop consists of iteratively executing a mixing process five items. The mixing process is illustrated in FIG. 10.

Referring now to FIG. 10, there is shown therein a schematic block diagram of the mixing process used in the authentication algorithm of the present invention. The mixing process 300 is provided with a first input of 16 key bytes and a second input of 16 input bytes. The 16 input bytes to the first iteration consist of the 4 bytes of RAND, 4 bytes of ESN and the 8 rolling key bytes Kb(0-7), in the following order:

RAND 4 bytes (a 16-bit RAND is repeated twice)
ESN 4 bytes
Kb(1)
Kb(2)
Kb(3)
Kb(4)
Kb(5)
Kb(6)
Kb(7)
Kb(0)

The 16 key bytes which are provided as input to each iteration of the mixing process are a cyclic selection from the 8 rolling key bytes Kb(0-7) and the 16 permanent key bytes Ka(0-15). In the first application of the algorithm, the order of use of the 16 key bytes is as follows:

Iteration number	Key bytes used
1	Ka(0) ---> Ka(15)
2	Kb(0) ---> Kb(7); Ka(0) ---> Ka(7)
3	Ka(8) ---> Ka(15); Kb(0) ---> Kb(7)
4	Kb(4) ---> Kb(7); Ka(0) ---> Ka(11)
5	Ka(4) ---> Ka(11); Kb(0) ---> Kb(3)

The above key sequences may be obtained simply by copying the key variables to a temporary memory area in the order Kb, Ka, Kb again, and selecting them sequentially from this memory starting at the appropriate place for each iteration.

Mixing Process of the Algorithm

The mixing process 300 combines the 16 key bytes and the 16 input bytes in pairs using, for example, byte-wide add instructions. The mixing process 300 also uses a random 1:1 substitution box or look-up table, referred to hereinafter as an S-Box, to convert a one byte value to another one byte value. The S-Box is preferably the same look-up table used by the keystream generator of the present system and discussed above in connection with FIGS. 5-6 as the source of the parameter R. The S-Box may be implemented by a 256-byte read-only memory (ROM) which may be included in microprocessor program memory. A 1:1 S-box means that every 8-bit input value produces a unique 8-bit output value, or stated differently, every possible 8-bit value occurs only once in the table. This is desirable in order to avoid an uneven distribution of values. In certain microprocessors, the programming task may be simplified if the S-box is configured to lie on a 256-byte page boundary so that addressing the S-box would require manipulation of the least significant address byte only.

Referring next to FIG. 11, a schematic block diagram of a building block or mixing cell of the mixing process may now be seen. The mixing process may be generally constructed from a plurality of mixing cells or inner loops of the type shown in FIG. 11. The particular mixing process 300 shown in FIG. 10 may be visualized as a vertical stack of 16 such mixing cells. Each of the cells is provided with one key byte and one input byte which are added together by an adder 310. The output of the adder 310 is used to address the contents of an S-box 320 which releases an output byte stored at the address defined by the output of the adder 310. A software implementation of the mixing cell

or inner loop is set forth below for both "Intel" and "Motorola" architecture microprocessors.

Second Application of the Algorithn

The second application of the algorithm generates a second group of 16 output bytes which may be used for the conversation key (S-key), and, if performed, update of the rolling key (B-key or Kb(0-7). The second application of the algorithm is exactly the same as the first application except for the order in which the key bytes and input bytes are used. In the second application of the algorithm, the order of use of the 16 key bytes is as follows:

Iteration number	Key bytes used
1	Kb(0) ---> Kb(7); Ka(0) ---> Ka(7)
2	Ka(8) ---> Ka(15); Kb(0) ---> Kb(7)
3	Kb(4) ---> Kb(7); Ka(0) ---> Ka(11)
4	Ka(4) ----> Ka(11); Kb(0) ---> Kb(3)
5	Ka(0) ---> Ka(15)

Additionally, the 16-byte input array is initialized using Ka bytes instead of Kb bytes as follows:

RAND(0)
RAND(1)
RAND(0)
RAND(1)
ESN(0)
ESN(1)
ESN(2)
ESN(3)
Ka(7)
Ka(8)
Ka(9)
Ka(10)
Ka(11)
Ka(12)
Ka(13)
Ka(14)

After executing all five iterations of the second application of the algorithm, the second 8 bytes appearing

in the 16-byte input array are used as the temporary enciphering variable (S-key) and the first 8 bytes become the next rolling key variable if an update of the rolling key is performed. In the event of a rolling key update, the first 8 output bytes overwrite the old rolling bytes in the order Kb(1), Kb(2), Kb(3), Kb(4), Kb(5), Kb(6), Kb(7), Kb(0).

The Contents of the S-Box

The contents of the S-box set forth below are exemplary only and are given in futher explanation of the authentication and encryption system of the present invention. As mentioned earlier, the S-Box used in the authentication algorithm may be the same as the R look-up table used in the encryption technique of the present invention. The contents of the S-box are expressed in hexadecimal notation below. The first byte (value=50) is in location 0, i.e, the beginning address of the ROM. The first line of data (16 values) is stored in locations 0 to 15 and subsequent lines of data are stored in the following 16 locations of the ROM, respectively.

ADDRESS	DATA
(00)	50 02 F1 C8 DE 21 OB 1C A5 F6 9A 61 10 4A 3C 34
(10)	CB F9 CO 77 20 B3 F5 6B E2 BC 69 71 EC 4B 48 85
(20)	5C 04 89 8C 76 13 CA 99 AD 5E 91 A0 9C B1 EA 2C
(30)	5F 94 97 06 4D AA 74 1B B8 B7 4C 65 35 ID 28 EF
(40)	E4 45 B6 6D J7 AE 5D 23 F4 CE E9 70 E8 64 54 F7
(50)	6A 22 8E AB 88 9F 26 57 32 E1 C2 E5 93 EB 6F 3F
(60)	A8 3B 41 47 25 D6 29 C3 OD C6 D7 8F 66 1A 68 8B
(70)	59 CD 80 BA 52 0A 1E 67 19 53 CF 30 2D 37 51 7C
(80)	42 B2 B0 A2 95 D4 B5 9E 73 8A 5A 56 60 9D A5 98
(90)	40 E3 49 OC C1 3E E6 7F 92 DF 33 A1 2F BE 3A 7E
(AO)	ED C5 F2 FD 03 BB 78 90 DB 7B E7 6E 2E C4 7A A9
(BO)	4F AF A7 96 38 81 24 87 FF B9 86 D8 58 CC D9 3D
(CO)	31 F3 62 9B FB OF 07 39 A6 D2 16 DD 43 63 DO FE
(DO)	82 D5 18 BF 12 01 6C A4 1F A3 8D 84 08 4E OE FA
(EO)	11 B4 C9 46 BD 14 2B 36 EE EO FC DC 7D 5B 72 D1
(FO)	55 2A 05 D3 27 44 AC DA 83 79 09 F8 75 C7 OO FO

Exemplary Coding For Common Types of Microprocessors

8080/8085 and Z80 Code

The fixed ROM or S-box is a 256-byte table located on a page boundary addressed by a 16-bit register DE.

```
CELMIX:  LDAX B    ;BC REGISTER IS USED TO POINT TO KEY
                   BYTES
         ADD  M    ;THE HL REGISTER POINTS TO INPUT BYTES
         MOV  E,A  ;THE SUM OF A KEY BYTE AND AN INPUT BYTE
         LDAX D    ;ADDRESSES THE S-BOX
         MOV  M,A  ;OUTPUT BYTE FROM S-BOX OVERWRITES INPUT
                   BYTE
         INX  H    ;NEXT INPUT BYTE ADDRESS
         INX  B    ;NEXT KEY BYTE ADDRESS
         RET
```

The above routine is used as follows:

(1) Set D register to MSB of S-box starting address which lies on a page boundary.

(2) Initialize BC to the appropriate starting address in the array of key bytes according to the iteration number as described previously.

(3) Initialize HL to point to the 16-byte array of input bytes.

(4) Execute routine 16 times.

The immediately preceding steps implement one iteration of the mixing process. Prior to the first iteration, the 16-byte input array is initialized with RAND, ESN and the above-indicated selection of A-key or B-key bytes.

The 16 output bytes lie in the original input byte array and are available for input to the next iteration. After performing all five iterations with the above-indicated selections of key bytes, the 16 output bytes represent the desired output of the algorithm.

Code for 6809

```
CELMIX:  LDA  ,X+  ;THE X REGISTER IS USED TO POINT TO
                       KEY BYTES
         ADDA ,Y   ;THE Y REGISTER POINTS TO INPUT
                   BYTES
         LDA  A,U  ;U=ADDRESS OF S-BOX START, A=OFFSET
                       FROM START
         STA  ,Y+  ;BYTE FROM S-BOX OVERWRITES INPUT
                   BYTE
                   RET
```

+ signifies autoincrement of indicated register after use

This routine is used as follows:

(1) Set U register to address to start of S-box.

(2) Initialize X register to point to appropriate key byte according to the order of use of key bytes described previously.

(3) Initialize Y register to point to the beginning of the 16-byte input byte array.

(4) Execute routine 16 times.

The immediately preceding steps implement one iteration of the mixing process illustrated in FIG. 10. Prior to the first iteration, the 16-byte input array is initialized with RAND, ESN and the specified selection of A-key or B-key bytes, as in the previous example. Hence, it is only necessary to re-initialize the Y register to the start of the input byte array and to re-initialize the X register to point to the appropriate key byte for each stage before executing the four remaining iterations. After the fifth iteration, the 16-byte input array contains the 16 output bytes from the first application of the algorithm which are used for authentication and, if implemented, subscriber identity masking.

It should be appreciated from the foregoing that a number of concepts are implemented in the system of the present invention. Among these concepts is the principle that some part of the authentication key (i.e., the "rolling key" part) should be periodically updated so that clones

would be required to track the history of the system. Bilateral authentication is used on the traffic channel to effect a rolling key update which is linked to a call counter update.

It may also be seen that execution of the authentication algorithm of the present invention also generates a temporary conversation key or "talk-variable" security key (S-key) which may be used for enciphering a subsequent call or group of calls and the actual secret permanent subscriber key (A-key) is never released by the home network. In addition, the algorithm of the present invention produces another output which may be used to mask the called subscriber identity.

The foregoing description shows only certain particular embodiments of the present invention. However, those skilled in the art will recognize that many modifications and variations may be made without departing substantially from the spirit and scope of the present invention. Accordingly, it should be clearly understood that the form of the invention described herein is exemplary only and is not intended as a limitation on the scope of the invention as defined in the following claims.

WHAT IS CLAIMED IS:

1. A method for the generation of a plurality of parameters for use in enhancing the security of communication in a digital cellular communications system in which each mobile station is assigned a unique multi-digit secret permanent key and in which a periodically changed multi-digit rolling key is employed for increased security, both said permanent key and said rolling key being stored in each mobile station and the home network of the mobile, said method comprising:

receiving at a location a plurality of multi-digit input signals, including, a signal representative of a random authentication inquiry from a visited network and a signal representative of a particular mobile station along with the multi-digit permanent key of said particular mobile station and the multi-digit rolling key associated with said particular mobile at that particular time;

arranging the digits of said input signals in a first grouping;

calculating from said first grouping of input signals and said permanent and rolling key digits a first output value in accordance with a first algorithm;

assigning sequentially arranged blocks of digits comprising said first output value to selected parameters for use within said system, including, an authentication response to be used by said mobile station to reply to the authentication inquiry by the visited network and an authentication signal to be used by the visited network to authenticate it to the mobile station;

arranging the digits of said input signals in a second grouping;

calculating from said said second grouping of input signals and said permanent and rolling key digits a second output value in accordance with a second algorithm; and

assigning sequentially arranged blocks of digits comprising said second output value to selected parameters for use within said system, including, a security key to be

used to calculating a keystream of pseuso-random bits for enciphering communications data within the system and a new rolling key to be associated with the particular mobile at a next particular time.

2. A method for the generation of a plurality of parameters for use in enhancing the security of communication in a digital cellular communications system as set forth in Claim 1 in which:

the output parameters for use within said system to which said sequentially arranged blocks of digits comprising said first output value are assigned also includes a signal to be used to mask the called number transmitted by the mobile station.

3. A method for the generation of a plurality of parameters for use in enhancing the security of communication in a digital cellular communications system as set forth in Claim 1 in which: said first and second algorithms comprise recursive executions of a code loop.

4. A method for the generation of a plurality of parameters for use in enhancing the security of communication in a digital cellular communications system as set forth in Claim 1 in which: said input signals and said key digits are grouped into bytes and said first and second algorithms comprise a mixing process in which respective pairs of bytes of input signals and key digits are iteratively added to one another.

5. A method for the generation of a plurality of parameters for use in enhancing the security of communication in a digital cellular communications system as set forth in Claim 1 in which: said method is executed in the home exchange of each mobile station.

6. A method for the generation of a plurality of parameters for use in enhancing the security of communication in a digital cellular communications system as set forth in Claim 4 in which: calculation in accordance with said first algorithm comprises grouping a sequence of bytes including said input signals and said rolling key digits and then mixing respective bytes thereof with bytes of said permanent key arranged in a first order by adding.

7. A method for the generation of a plurality of parameters for use in enhancing the security of communication in a digital cellular communications system as set forth in Claim 6 in which: calculation in accordance with said second algorithm comprises grouping a sequence of bytes including said input signals and said rolling key digits and then mixing respective bytes thereof with bytes of said permanent key arranged in a second order, different from said first order, by adding.

8. A method for the generation of a plurality of parameters for use in enhancing the security of communication in a digital cellular communications system as set forth in Claim 4 in which: the value obtained from each addition is used to obtain a random number from a fixed look-up table having a 1:1 mapping between its input and its output.

9. A method for the generation of a plurality of parameters for use in enhancing the security of communication in a digital cellular communications system as set forth in Claim 4 in which: said fixed look-up table is also used to obtain random numbers for use in an algorithm for generating a psuedo-random keystream for enciphering communications data withing said system.

10. A system for the generating a plurality of parameters for use in enhancing the security of

communication in a digital cellular communications system in which each mobile station is assigned a unique multi-digit secret permanent key and in which a periodically changed multi-digit rolling key is employed for increased security, both said permanent key and said rolling key being stored in each mobile station and the home network of the mobile, said method comprising:

means for receiving at a location a plurality of mult-digit input signals, including, a signal representative of a random authentication inquiry from a visited network, and a signal representative of a particular mobile station along with the multi-digit permanent key of said particular mobile station, and the multi-digit rolling key associated with said particular mobile at that particular time;

means for arranging the digits of said input signals in a first grouping;

means for calculating from said first grouping of input signals and said permanent and rolling key digits a first output value in accordance with a first algorithm;

means for assigning sequentially arranged blocks of digits comprising said first output value to selected parameters for use within said system, including, an authentication response to be used by said mobile station to reply to the authentication inquiry by the visited network and an authentication signal to be used by the visited network to authenticate it to the mobile station;

means for arranging the digits of said input signals in a second grouping;

means for calculating from said second grouping of input signals and said permanent and rolling key digits a second output value in accordance with a second algorithm; and

means for assigning sequentially arranged blocks of digits comprising said second output value to selected parameters for use within said system, including, a security key to be used to calculating a keystream of pseuso-random bits for enciphering communications data within the system

and a new rolling key to be associated with the particular mobile at a next particular time.

11. A system for generating a plurality of parameters for use in enhancing the security of communication in a digital cellular communications system as set forth in Claim 10 in which:

the output parameters for use within said system to which said sequentially arranged blocks of digits comprising said first output value are assigned also includes a signal to be used to mask the called number transmitted by the mobile station.

12. A system for the generating a plurality of parameters for use in enhancing the security of communication in a digital cellular communications system as set forth in Claim 10 in which:

said first and second algorithms comprise recursive executions of a code loops.

13. A system for generating a plurality of parameters for use in enhancing the security of communication in a digital cellular communications system as set forth in Claim 10 in which:

said input signals and said key digits are grouped into bytes and said first and second algorithms comprise a mixing process in which respective pairs of bytes of input signals and key digits are iteratively added to one another.

14. A system for generating a plurality of parameters for use in enhancing the security of communication in a digital cellular communications system as set forth in Claim 10 which also includes:

means for implementing said systen in the home exchange of each mobile station.

15. A system for generating a plurality of parameters for use in enhancing the security of communication in a digital cellular communications system as set forth in Claim 13 in which:

said means for calculation in accordance with said first algorithm comprises means for grouping a sequence of bytes including said input signals and said rolling key digits and then mixing respective bytes thereof with bytes of said permanent key aranged in a first order by adding.

16. A system for generating a plurality of parameters for use in enhancing the security of communication in a digital cellular communications system as set forth in Claim 15 in which:

said means for calculation in accordance with said second algorithm comprises means for grouping a sequence of bytes including said input signals and said rolling key digits and then mixing respective bytes thereof with bytes of said permanent key aranged in a second order, different from said first order, by adding.

17. A system for generating a plurality of parameters for use in enhancing the security of communication in a digital cellular communications system as set forth in Claim 13 in which: the value obtained from each addition is used to obtain a random number from a fixed look-up table having a 1:1 mapping between its input and its output.

18. A system for generating a plurality of parameters for use in enhancing the security of communication in a digital cellular communications system as set forth in Claim 17 in which: said fixed look-up table is also used to obtain random numbers for use in an algorithm for generating a psuedo-random keystream for enciphering communications data withing said system.

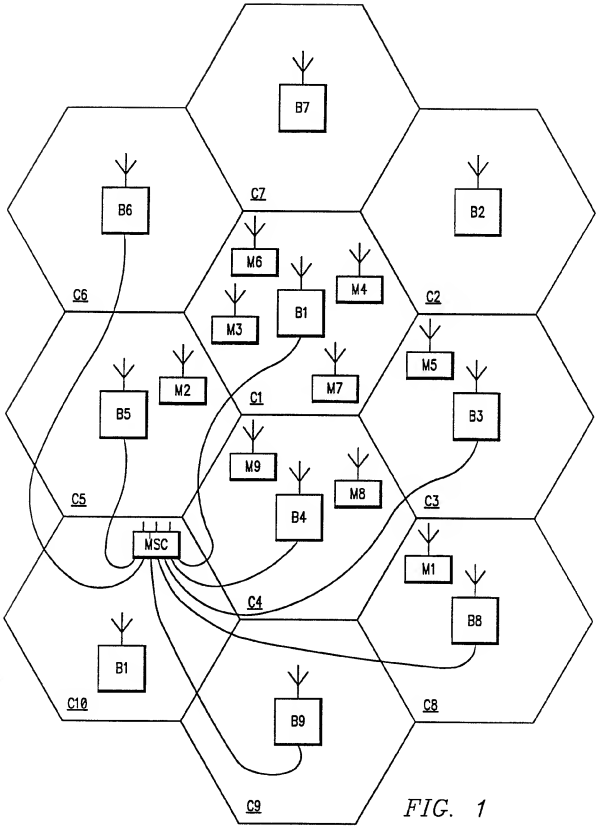

B7
B6
C7
B2
M6
M4
C6
C2
M3
B1
M5
M2
M7
C1
B5
B3
M9
M8
C5
B4
C3
MSC
M1
C4
B8
B1
C10
B9
C8
C9

FIG. 1

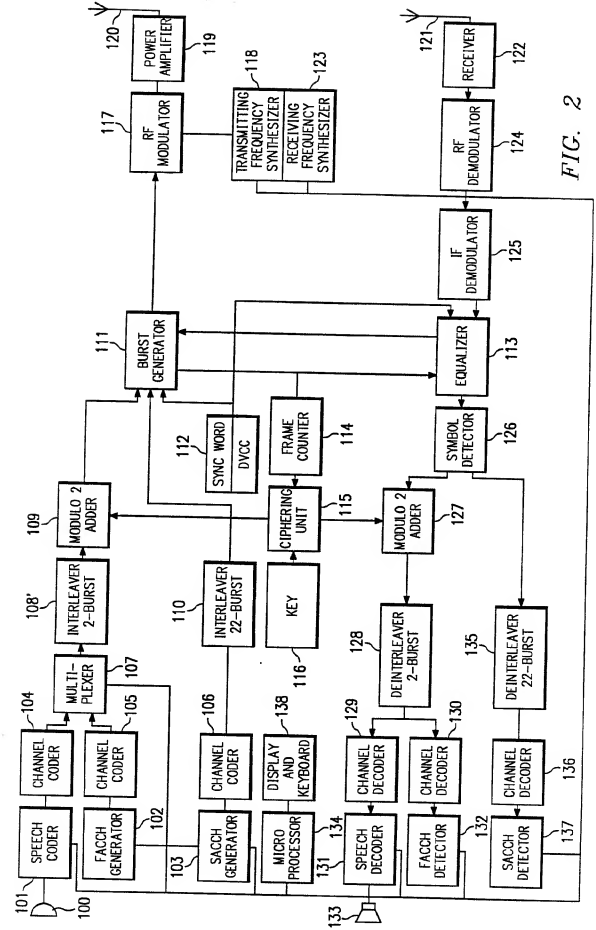

SPEECH CODER
FACCH GENERATOR
SACCH GENERATOR
MICRO PROCESSOR
CHANNEL CODER
CHANNEL CODER
CHANNEL CODER
DISPLAY AND KEYBOARD
MULTI-PLEXER
INTERLEAVER 2-BURST
INTERLEAVER 22-BURST
KEY
MODULO 2 ADDER
CIPHERING UNIT
SYNC WORD
DVCC
FRAME COUNTER
BURST GENERATOR
RF MODULATOR
POWER AMPLIFIER
TRANSMITTING FREQUENCY SYNTHESIZER
RECEIVING FREQUENCY SYNTHESIZER
RECEIVER
RF DEMODULATOR
IF DEMODULATOR
EQUALIZER
SYMBOL DETECTOR
MODULO 2 ADDER
DEINTERLEAVER 2-BURST
DEINTERLEAVER 22-BURST
CHANNEL DECODER
CHANNEL DECODER
CHANNEL DECODER
SPEECH DECODER
FACCH DETECTOR
SACCH DETECTOR
100
101
102
103
104
105
106
107
108'
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138

FIG. 2

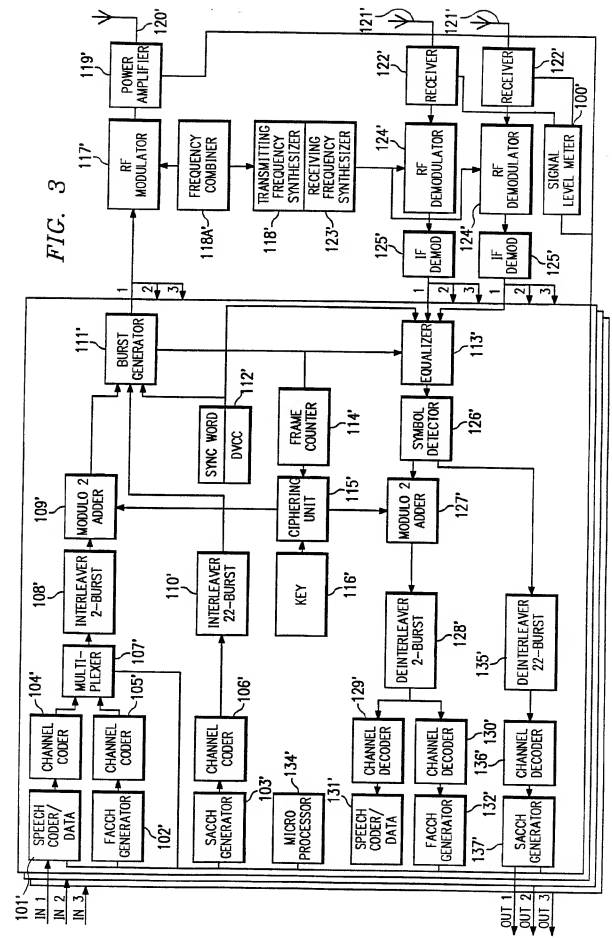
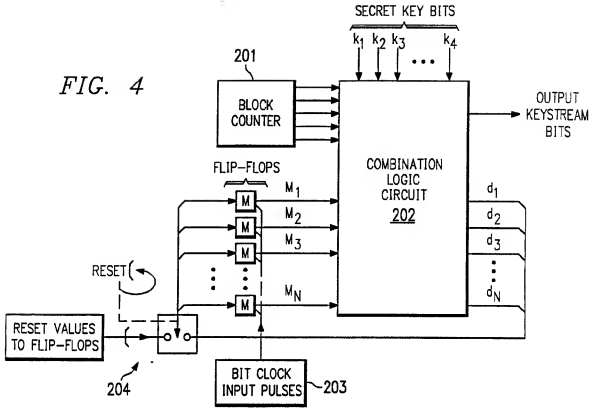

101'
IN 1
IN 2
IN 3
SPEECH CODER/ DATA
FACCH GENERATOR
SACCH GENERATOR
MICRO PROCESSOR
CHANNEL CODER
CHANNEL CODER
CHANNEL CODER
MULTI-PLEXER
INTERLEAVER 2-BURST
INTERLEAVER 22-BURST
KEY
MODULO 2 ADDER
CIPHERING UNIT
SYNC WORD
DVCC
FRAME COUNTER
BURST GENERATOR
RF MODULATOR
FREQUENCY COMBINER
TRANSMITTING FREQUENCY SYNTHESIZER
RECEIVING FREQUENCY SYNTHESIZER
POWER AMPLIFIER
RECEIVER
RECEIVER
RF DEMODULATOR
RF DEMODULATOR
SIGNAL LEVEL METER
IF DEMOD
IF DEMOD
EQUALIZER
SYMBOL DETECTOR
MODULO 2 ADDER
DEINTERLEAVER 2-BURST
DEINTERLEAVER 22-BURST
CHANNEL DECODER
CHANNEL DECODER
CHANNEL DECODER
SPEECH CODER/ DATA
FACCH GENERATOR
SACCH GENERATOR
OUT 1
OUT 2
OUT 3

FIG. 3

FIG. 4


SECRET KEY BITS
k_1 k_2 k_3 ... k_4
201
BLOCK COUNTER
OUTPUT KEYSTREAM BITS
FLIP-FLOPS
COMBINATION LOGIC CIRCUIT
202
M_1
M_2
M_3
M_N
d_1
d_2
d_3
d_N
RESET
RESET VALUES TO FLIP-FLOPS
204
BIT CLOCK INPUT PULSES
203

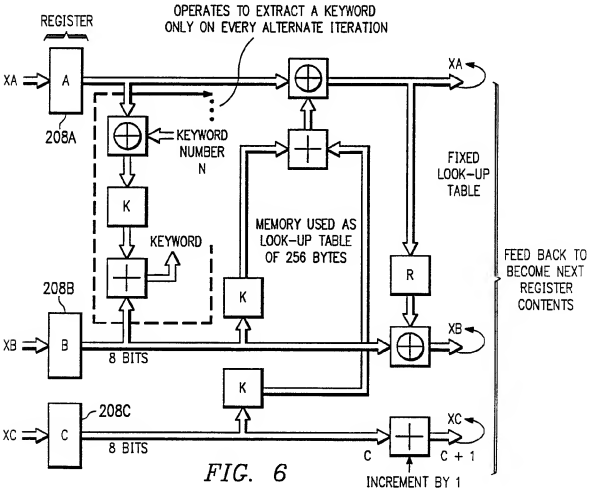
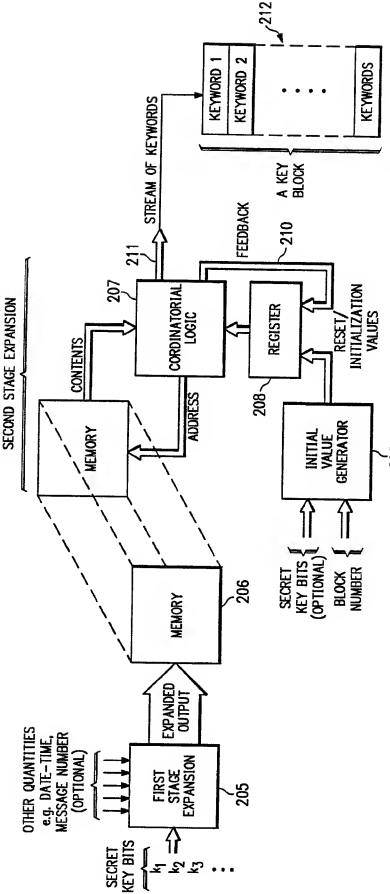

REGISTER
OPERATES TO EXTRACT A KEYWORD ONLY ON EVERY ALTERNATE ITERATION
XA
A
208A
KEYWORD NUMBER N
K
KEYWORD
MEMORY USED AS LOOK-UP TABLE OF 256 BYTES
FIXED LOOK-UP TABLE
R
FEED BACK TO BECOME NEXT REGISTER CONTENTS
208B
XB
B
8 BITS
XC
C
208C
8 BITS
C
C + 1
INCREMENT BY 1

FIG. 6

FIG. 5


SECRET KEY BITS
k1
k2
k3
OTHER QUANTITIES e.g. DATE-TIME, MESSAGE NUMBER (OPTIONAL)
FIRST STAGE EXPANSION
205
EXPANDED OUTPUT
MEMORY
206
SECOND STAGE EXPANSION
MEMORY
CONTENTS
ADDRESS
207
CORDINATORIAL LOGIC
211
STREAM OF KEYWORDS
212
KEYWORD 1
KEYWORD 2
KEYWORDS
A KEY BLOCK
FEEDBACK
210
REGISTER
208
RESET/ INITIALIZATION VALUES
INITIAL VALUE GENERATOR
209
SECRET KEY BITS (OPTIONAL)
BLOCK NUMBER

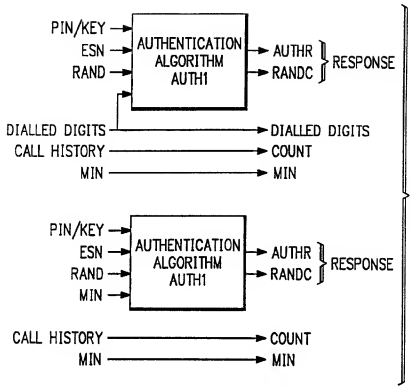


FIG. 7
(PRIOR ART)

FIG. 8

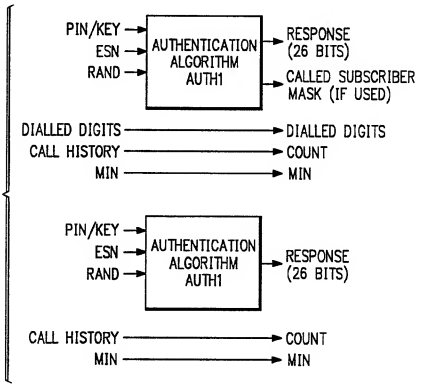
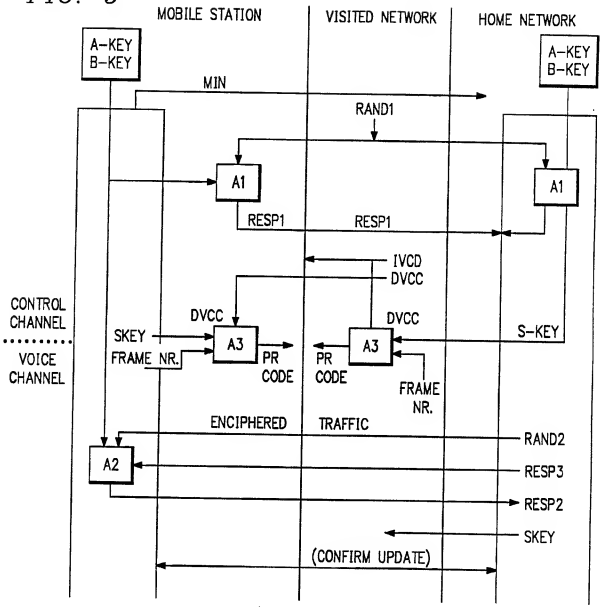


FIG. 9



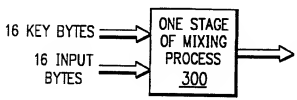
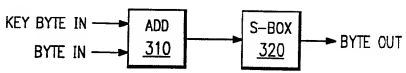


FIG. 10

FIG. 11



INTERNATIONAL SEARCH REPORT

International Application No. PCT/US91/05078

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [6]

According to International Patent Classification (IPC) or to both National Classification and IPC

IPC(5): H04L 9/00
US. CL.: 380/46

II. FIELDS SEARCHED

Minimum Documentation Searched [7]	
Classification System	Classification Symbols
	380/21,23,28,43,44,46,47,48,49,50 455/33 375/107,110,112
US. CL.	370/103,105,107 379/59,60

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched [8]

III. DOCUMENTS CONSIDERED TO BE RELEVANT [9]

Category *	Citation of Document, [11] with indication, where appropriate, of the relevant passages [12]	Relevant to Claim No. [13]
A	4,876,740 (LEVINE ET AL) 24 OCTOBER 1989 SEE FIGURE 24	1-18
A	4,914,696 (DUDCZAK ET AL) 03 APRIL 1990 SEE FIGURE 4	1-18
A	4,827,507 (MARRY ET AL) 02 MAY 1989 SEE FIGURE 6	1-18
A	4,549,308 (LoPINTO) 22 OCTOBER 1985, SEE FIGURE 3	1-18

* Special categories of cited documents: [10]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
21 AUGUST 1991	29 AUG 1991
International Searching Authority	Signature of Authorized Officer
ISA/US	TOD SWANN

Form PCT/ISA/210 (second sheet) (Rev.11-87)